GETVPN Backup Network Deployment Guide

This document is solution deployment guide for GDOI encryption in secondary network. Deployment of the following two solution test cases are covered in this document:

1. Use same GDOI policies for both primary and secondary Service Provider (SP) network paths in the Group Member (GM). PPPoE Secondary SP network path and DMVPN Secondary SP path are covered in this document.
2. Use different GDOI group for each SP network path with redundancy where even the crypto services are disjoint.

Contents

1. GETVPN Backup Network Solution Objectives

Following solution test cases are covered in this document:

- **Same GDOI (Group Domain of Interpretation) group and policies for both networks:** Use same GDOI policies for both primary and secondary Service Provider (SP) network paths in the Group Member (GM). This case is required if the enterprise VPN spans both providers (e.g. Inter-Provider Inter-AS MPLS VPN). When a GM's path via the primary MPLS network fails, routes are converged in the GM, and GM uses secondary (SP) path to reach other GMs. The GM's traffic may pass through the Inter-Provider Inter-AS link to reach other GM's attached to the primary SP network. In this case, all GM use same GDOI policies on all possible paths. Encrypted traffic flow high availability is achieved via route convergence. Generally, the shortest path between two GM dual-homed to two SP networks will be via the same SP network. There are cases where one GM has a failure to the primary network while another GM has a failure to the secondary network. Traffic between these GM must pass via the Inter-provider Inter-AS link.
- **Failure:** Outage of a GM link to the primary SP network.
- **Recovery:** Route convergence and traffic flow via Secondary SP network in the GM.

Solution test for this case is provided in section 2.

- **Use different GDOI group for each SP network path:** This case is needed if the user wants independent redundancy where even the crypto services are disjoint. The provider VPN networks MUST be disjoint in this case. Different GDOI group is used for each SP network path in the GM. GM High Availability is achieved by triggering EEM script to filter primary network routes if crypto failure is incurred so traffic may traverse through the secondary network.
- **Failure:** Primary SP routes are fine. But GM is unable to register to Key Server (KS) and unable to receive rekeys from the KS. These are typically operator errors. For example pre-shared keys are not matching between KS and GM or ACL is dropping rekey packets or rekeys are not received in GM due to multicast problem.
- **Recovery:** After GM registration failure to the last KS, trigger EEM script to filter all primary network routes except routes to the KS. This will cause route convergence to occur and induce GM traffic to be sent via secondary SP network with different keys. This is done in order to insure the routes are revoked on the primary provider network where the crypto has failed.

Solution test case for this case is provided in Section 3.

2. Using GETVPN in PPPoE Secondary SP Network

2.1 Objective

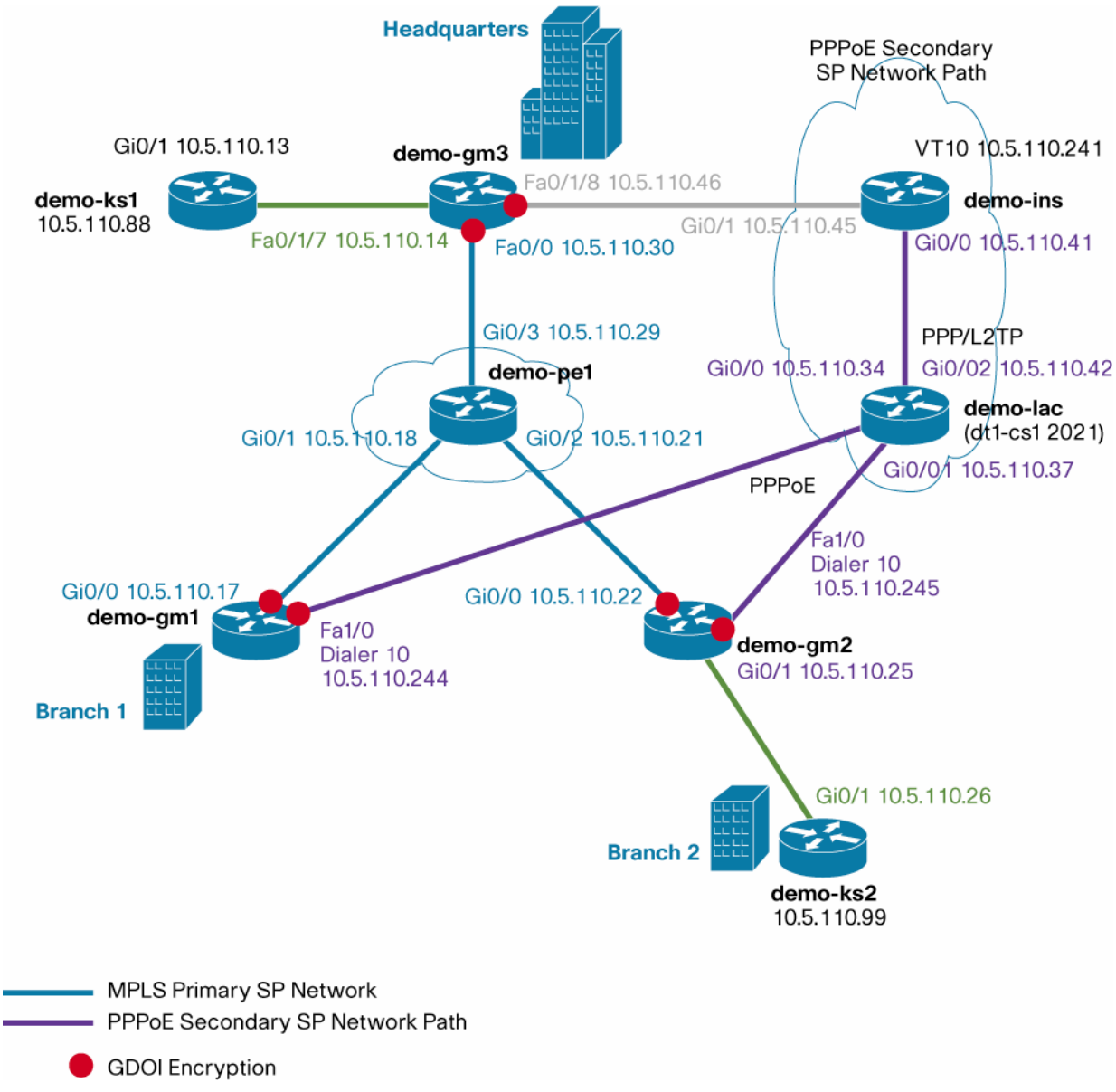
Following are objectives of the solution test.

- **Test GDOI encryption of traffic via PPPoE network.**
- **Test failover of primary SP network.** When primary SP network fails, traffic will flow through the secondary SP network. When the primary SP network is restored, traffic will switch back to primary SP network from the secondary SP network.

2.2 Solution Test Topology

GETVPN solution test setup consists of three GMs (Group Members) and two KS (Key Server) are included in the setup. “demo-pe1” simulates the MPLS primary SP network. One Key server is located in the Headquarters. Other Key server is connected behind GM in one of the branch.

Figure 1. Demo GETVPN Network Topology



GMs between branches and headquarters are also connected via secondary PPPoE service provider network. This secondary network will be used when there is network outage in primary SP network. GM between branches are connected to demo-lac via PPPoE interface. PPPoL2TP tunnel connects between demo-lac and demo-lns.

GDOI encryption is done on the customer network side in the GM routers. Traffic flowing through the interface connected to primary SP network and the interface connected to the secondary service provider network are GDOI encrypted.

2.3 PPPoE Secondary SP Network Configuration

Following sections provide PPPoE configuration commands needed for provisioning PPPoE secondary SP network in the solution test setup.

2.3.1 Configuration of GM in Branch 1 (demo-gm1)

Following lists PPPoE related configuration in demo-gm1:

```
aaa new-model
!
aaa authentication ppp default local
!
bba-group pppoe global
!
username demo password lab
!
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet1/0
 description connected to demo-lac
 no switchport
 no ip address
 ip pim sparse-mode
 ip tcp adjust-mss 1452
 pppoe enable group global
 pppoe-client dial-pool-number 10
!
interface Vlan10
 ip address 10.5.110.201 255.255.255.248
 ip pim sparse-mode
 ip igmp join-group 239.192.1.190 source 10.5.110.88
 ip igmp join-group 239.192.1.190 source 10.5.110.99
 no autostate
!
interface Dialer10
 ip address negotiated
 ip mtu 1492
 ip pim sparse-mode
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip mroute-cache
```

```
 dialer pool 10
 ppp authentication pap
 ppp pap sent-username demo@cisco.com password lab
 crypto map gdoi
!
router eigrp 44
 network 10.5.110.12 0.0.0.3
 network 10.5.110.16 0.0.0.3
 network 10.5.110.200 0.0.0.7
 network 10.5.110.240 0.0.0.7
 no auto-summary
!
ip nat inside source list 10 interface Dialer10 overload
!
access-list 10 permit 10.5.110.200 0.0.0.7
dialer-list 10 protocol ip list 10
```

2.3.2 Configuration of GM in Branch 2 (demo-gm2)

Following lists PPPoE related configuration in demo-gm2:

```
aaa new-model
!
aaa authentication ppp default local
!
bba-group pppoe global
!
username demo password lab
!
interface FastEthernet1/0
 description connected to demo-lac
 no switchport
 no ip address
 ip pim sparse-mode
 ip tcp adjust-mss 1452
 pppoe enable group global
 pppoe-client dial-pool-number 10
!
interface Vlan10
 ip address 10.5.110.209 255.255.255.248
 ip pim sparse-mode
 ip nat inside
 ip virtual-reassembly
 ip tcp adjust-mss 1452
 ip igmp join-group 239.192.1.190 source 10.5.110.88
 ip igmp join-group 239.192.1.190 source 10.5.110.99
 no ip mroute-cache
 no autostate
!
interface Dialer10
 ip address negotiated
```

```
 ip mtu 1492
 ip pim sparse-mode
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip mroute-cache
 dialer pool 10
 ppp authentication pap
 ppp pap sent-username demo@cisco.com password lab
 crypto map gdoi
!
router eigrp 44
 network 10.5.110.20 0.0.0.3
 network 10.5.110.24 0.0.0.3
 network 10.5.110.208 0.0.0.7
 network 10.5.110.240 0.0.0.7
 no auto-summary
!
ip nat inside source list 10 interface Dialer10 overload
!
access-list 10 permit 10.5.110.208 0.0.0.7
dialer-list 10 protocol ip list 10
```

2.3.3 Configuration of GM in Headquarters (demo-gm3)

Following lists PPPoE path related configuration in demo-gm3:

```
username demo password lab
!
interface FastEthernet0/1/8
 switchport access vlan 20
!
interface Vlan20
 ip address 10.5.110.46 255.255.255.252
 ip pim sparse-mode
 no autostate
 crypto map gdoi
!
router eigrp 44
 redistribute static
 network 10.5.110.8 0.0.0.3
 network 10.5.110.12 0.0.0.3
 network 10.5.110.28 0.0.0.3
 network 10.5.110.44 0.0.0.3
 network 10.5.110.216 0.0.0.7
 no auto-summary
```

2.3.4 Configuration of LAC in SP Network (demo-lac)

Following lists PPPoE related configuration in demo-lac:

```
aaa new-model
```

```
!
aaa authentication ppp default local
!
vpdn enable
!
vpdn-group demo-getvpn-pppoe
! Default L2TP VPDN group
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.5.110.41
 local name demo-lac
 l2tp tunnel password lab
!
bba-group pppoe demo-getvpn-pppoe
 virtual-template 11
 sessions auto cleanup
!
interface GigabitEthernet0/0
 description connected to demo-gm1
 ip address 10.5.110.34 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 pppoe enable group demo-getvpn-pppoe
!
interface GigabitEthernet0/1
 description connected to demo-gm2
 ip address 10.5.110.37 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 pppoe enable group demo-getvpn-pppoe
!
interface GigabitEthernet0/2
 description connected to LNS
 ip address 10.5.110.42 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface Virtual-Template11
 no ip address
 ip mtu 1492
```

```
 no ip route-cache cef
 ppp authentication pap
 ppp pap sent-username demo password lab
!
router eigrp 44
 network 10.5.110.32 0.0.0.3
 network 10.5.110.36 0.0.0.3
 network 10.5.110.40 0.0.0.3
 network 10.5.110.240 0.0.0.7
 no auto-summary
```

2.3.5 Configuration of LNS in SP Network (demo-lns)

Following lists PPPoE related configuration in demo-lns:

```
aaa new-model
!
aaa authentication ppp default local
!
vpdn enable
!
vpdn-group demo-getvpn-pppoe
 accept-dialin
  protocol l2tp
  virtual-template 10
 terminate-from hostname demo-lac
 local name demo-lns
 l2tp tunnel password lab
!
username demo@cisco.com password lab
username demo password lab
!
interface GigabitEthernet0/0
 ip address 10.5.110.41 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 ip address 10.5.110.45 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 media-type rj45
!
interface Virtual-Template10
 ip unnumbered GigabitEthernet0/0
 ip mtu 1492
 ip pim sparse-mode
 no ip route-cache cef
```

```
 peer default ip address pool l2tp-pool
 ppp authentication pap
 ppp pap sent-username demo password 7 060A0E23
!
router eigrp 44
 network 10.5.110.40 0.0.0.3
 network 10.5.110.44 0.0.0.3
 network 10.5.110.240 0.0.0.7
 no auto-summary
!
ip local pool l2tp-pool 10.5.110.242 10.5.110.246
```

2.4 PPPoE Secondary SP Network Verification

Following sections provide verification of PPPoE secondary SP network functionality in the solution test setup.

2.4.1 Verification of PPPoE Path Setup

On user router (**client**) enable the following debug commands:

```
Debug ppp negotiation
Debug ppp authentication
Debug pppoe events
Debug pppoe errors
```

On **LAC** and **LNS** enable the following debug commands:

```
Debug ppp negotiation
Debug ppp authentication
Debug pppoe events
Debug pppoe error
Debug sss event
Debug sss error
Debug vpdn events
Debug vpdn errors
Debug vpdn l2x-events
Debug vpdn l2x-errors
```

Client demo-gm2:

```
*Feb  4 14:44:15:  Sending PADI: Interface = FastEthernet1/0
*Feb  4 14:44:15: PPPoE 0: I PADO  R:0013.5f52.601a L:0013.1a1c.e1a6 Fa1/0sh
*Feb  4 14:44:17:  PPPOE: we've got our pado and the pado timer went off
*Feb  4 14:44:17: OUT PADR from PPPoE Session
*Feb  4 14:44:17: PPPoE 217: I PADS  R:0013.5f52.601a L:0013.1a1c.e1a6 Fa1/0
*Feb  4 14:44:17: IN PADS from PPPoE Session
*Feb  4 14:44:17: %DIALER-6-BIND: Interface Vi2 bound to profile Di10
*Feb  4 14:44:17: PPPoE: Virtual Access interface obtained.
*Feb  4 14:44:17: PPPoE : encap string prepared
*Feb  4 14:44:17: Vi2 LCP: State is Open
*Feb  4 14:44:17: Vi2 PPP: Phase is AUTHENTICATING, Authenticated User
*Feb  4 14:44:17: Vi2 DDR: Remote name for cisco
*Feb  4 14:44:17: Vi2 PAP: O AUTH-ACK id 1 len 5
```

```
*Feb  4 14:44:17: Vi2 PPP: Phase is UP
*Feb  4 14:44:17: Vi2 IPCP: State is Open
*Feb  4 14:44:17: Di10 IPCP: Install negotiated IP interface address 10.5.110.243
Dialer10                   10.5.110.243    YES IPCP   up                    up
```

LAC demo-lac:

```
Feb 16 23:18:47.651: PPPoE 0: O PADO, R:0013.5f52.601b L:000f.8fcf.a83d Gi0/0
Feb 16 23:18:47.651:  Service tag: NULL Tag
Feb 16 23:18:49.699: PPPoE 0: I PADR  R:000f.8fcf.a83d L:0013.5f52.601b Gi0/0
Feb 16 23:18:49.699:  Service tag: NULL Tag
Feb 16 23:18:49.699: PPPoE : encap string prepared
Feb 16 23:18:49.699: [179]PPPoE 165: Service request sent to SSS
Feb 16 23:18:49.699: [179]PPPoE 165: Created, Service: None R:0013.5f52.601b
L:000f.8fcf.a83d Gi0/0
Feb 16 23:18:49.703: ppp179 PPP: Send Message[Dynamic Bind Response]
Feb 16 23:18:49.703: ppp179 PPP: Using vpn set call direction
Feb 16 23:18:49.703: ppp179 PPP: Treating connection as a callin
Feb 16 23:18:49.703: ppp179 PPP: Session handle[6100010E] Session id[179]
Feb 16 23:18:49.703: ppp179 PPP: Phase is ESTABLISHING, Passive Open
Feb 16 23:18:49.703: ppp179 LCP: State is Listen
Feb 16 23:18:49.703: [179]PPPoE 165: State PPP_START    Event DYN_BIND
Feb 16 23:18:49.703: [179]PPPoE 165: data path set to PPP
Feb 16 23:18:49.707: ppp179 LCP: I CONFREQ [Listen] id 1 len 14
Feb 16 23:18:49.707: ppp179 LCP:    AuthProto PAP (0x0304C023)
Feb 16 23:18:49.711: ppp179 LCP: State is Open
Feb 16 23:18:49.711: ppp179 PPP: Phase is AUTHENTICATING, by both
Feb 16 23:18:49.711: ppp179 PAP: I AUTH-REQ id 1 len 24 from "cisco@cisco.com"
Feb 16 23:18:49.711: ppp179 PAP: Authenticating peer cisco@cisco.com
Feb 16 23:18:49.711: ppp179 PPP: Phase is FORWARDING, Attempting Forward
Feb 16 23:18:49.715: [179]PPPoE 165: Access IE nas port called
Feb 16 23:18:49.715: [179]PPPoE 165: State LCP_NEGOTIATION    Event PPP_FWDING
Feb 16 23:18:49.727: SSS MGR [uid:179]: Handling Service-Connected event
Feb 16 23:18:49.727: ppp179 PPP SSS: Receive SSS-Mgr Forwarded
Feb 16 23:18:49.727: ppp179 PPP: Phase is FORWARDED, Session Forwarded
Feb 16 23:18:49.727: ppp179 PPP: Send Message[Forwarded]
Feb 16 23:18:49.731: [179]PPPoE 165: State LCP_NEGOTIATION    Event PPP_FWDED
Feb 16 23:18:49.731: [179]PPPoE 165: data path set to SSS Switch
Feb 16 23:18:49.731: [179]PPPoE 165: Connected Forwarded
```

LNS demo-lac#:

```
*Feb 16 23:19:45.371: L2TP _____:_____:________:     remote ip set to 10.5.110.42
*Feb 16 23:19:45.371: L2TP _____:_____:________:     local ip set to 10.5.110.41
*Feb 16 23:19:45.371: L2TP tnl   01012:0000B65B: FSM-CC ev Session-Conn
*Feb 16 23:19:45.371: L2TP tnl   01012:0000B65B: FSM-CC    in established
*Feb 16 23:19:45.371: L2TP tnl   01012:0000B65B: FSM-CC do Session-Conn-Est
*Feb 16 23:19:45.371: L2TP tnl   01012:0000B65B:   Session count now 2
*Feb 16 23:19:45.371: L2TP _____:01012:0000001C: FSM-Sn ev CC-Up
*Feb 16 23:19:45.375: L2TP _____:01012:0000001C:   App type set to VPDN
*Feb 16 23:19:45.383: L2TP _____:01012:0000001C: FSM-Sn do Established
```

```
*Feb 16 23:19:45.383: L2TP _____:01012:0000001C: Session up
*Feb 16 23:19:45.383: L2TP _____:01012:0000001C:   10.5.110.41<->10.5.110.42
*Feb 16 23:19:45.383: L2X:Session DB (Tnl/Sn: 46683/28): Stored the switching
session in the session DB
*Feb 16 23:19:45.383: L2TP:(Tnl46683:Sn28)Provisioned: idb=none,
session_sip=1,idb_switching=0, sw_mode=1
*Feb 16 23:19:45.383: L2TP:(Tnl46683:Sn28)L2X s/w switching session provisioned
*Feb 16 23:19:45.383: VPDN Received L2TUN socket message <xCCN - Session Connected>
*Feb 16 23:19:45.383: VPDN uid:27 VPDN session up
*Feb 16 23:19:45.383: SSS INFO: Element type is Tunnel-Name, string value is demo-
lac
*Feb 16 23:19:45.383: SSS MGR [uid:27]: Handling Policy Authorize (1 pending
sessions)
*Feb 16 23:19:45.387: ppp27 PPP: Phase is ESTABLISHING
*Feb 16 23:19:45.387: ppp27 PPP: Send Message[Dynamic Bind Response]
*Feb 16 23:19:45.387: ppp27 LCP: I FORCED rcvd CONFACK len 14
*Feb 16 23:19:45.387: ppp27 LCP:    MRU 1500 (0x010405DC)
*Feb 16 23:19:45.387: ppp27 LCP:    AuthProto PAP (0x0304C023)
*Feb 16 23:19:45.387: ppp27 PPP: Phase is FORWARDING, Attempting Forward
*Feb 16 23:19:45.387: ppp27 PPP: Phase is FORWARDING, Attempting Forward
*Feb 16 23:19:45.387: ppp27 PPP: Send Message[Connect Local]
*Feb 16 23:19:45.399: Vi4 PPP: Phase is DOWN, Setup
*Feb 16 23:19:45.399: VPDN uid:27 Virtual interface created for cisco@cisco.com
bandwidth
h 100000 Kbps
*Feb 16 23:19:45.399: VPDN Vi4 Virtual interface created for cisco@cisco.com,
bandwidth 100000 Kbps
*Feb 16 23:19:45.399: VPDN Vi4 Setting up dataplane for L2-L3, Vi4
*Feb 16 23:19:45.403: %LINK-3-UPDOWN: Interface Virtual-Access4, changed state to
up
*Feb 16 23:19:45.403: Vi4 PPP: Phase is AUTHENTICATING, Authenticated User
*Feb 16 23:19:47.411: Vi4 IPCP: Pool returned 10.5.110.243
*Feb 16 23:19:47.411: Vi4 IPCP: State is Open
L2X_ADJ: Vi4:adj notify change, event 2
L2X_ADJ: Vi4:midchain stacking IP 0.0.0.0 to 10.5.110.42 (VRF 0)
L2X_ADJ: Vi4:adj notify change, event 8
L2X_ADJ: Vi4:adj notify change, event 3
*Feb 16 23:19:47.411: Vi4 IPCP: Install route to 10.5.110.243
*Feb 16 23:19:47.423: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 44: Neighbor 10.5.110.243
(Virtual-Access4) is up: new adjacency
```

2.4.2 Verify PPPoE Session between the Branch and LNS

Following lists CLI commands to verify PPPoE session between the branch and LNS.

```
demo-gm1#show pppoe session
     1 client session
Uniq ID  PPPoE  RemMAC          Port                 Source   VA         State
           SID  LocMAC                                        VA-st
    N/A    171  0013.5f52.601b  Fa1/0                Di10     Vi2        UP
                000f.8fcf.a83d                                UP
demo-gm1#show users
    Line       User       Host(s)              Idle       Location
```

```
*  0 con 0               idle                 00:00:00

  Interface    User               Mode         Idle     Peer Address
  Vi2          demo               PPPoE        00:00:04 10.5.110.41
```

```
demo-lac#show vpdn session

L2TP Session Information Total tunnels 1 sessions 2

LocID      RemID      TunID      Username, Intf/      State  Last Chg Uniq ID
                                 Vcid, Circuit
31         33         50032      demo@cisco.co, Gi0/1 est    00:04:40 184
32         34         50032      demo@cisco.co, Gi0/0 est    00:04:40 185
```

```
demo-lac#show vpdn tunnels

L2TP Tunnel Information Total tunnels 1 sessions 2

LocTunID   RemTunID   Remote Name   State  Remote Address  Sessn L2TP Class/
                                                          Count VPDN Group
50032      13621      demo-lns      est    10.5.110.41     2     demo-getvpn-ppp
```

```
demo-lac#show pppoe sessions
     2 sessions in FORWARDED (FWDED) State
     2 sessions total

Uniq ID  PPPoE  RemMAC          Port                 Source   VA         State
           SID  LocMAC                                       VA-st
    185    171  000f.8fcf.a83d  Gi0/0                Vt11     N/A        FWDED
                0013.5f52.601b
    184    170  0013.1a1c.e1a6  Gi0/1                Vt11     N/A        FWDED
                0013.5f52.601a
```

```
demo-lns#show pppoe sessions

Uniq ID  PPPoE  RemMAC          Port                 Source   VA         State
           SID  LocMAC                                       VA-st
```

```
demo-lns#show vpdn sessions

L2TP Session Information Total tunnels 1 sessions 2

LocID      RemID      TunID      Username, Intf/      State  Last Chg Uniq ID
                                 Vcid, Circuit
33         31         13621      demo@cisco.com, Vi4  est    00:12:22 32
34         32         13621      demo@cisco.com, Vi5  est    00:12:21 33
```

```
demo-lns#show vpdn tunnels
```

```
L2TP Tunnel Information Total tunnels 1 sessions 2

LocTunID   RemTunID   Remote Name   State  Remote Address  Sessn L2TP Class/
                                                          Count VPDN Group
13621      50032      demo-lac      est    10.5.110.42     2     demo-getvpn-ppp

demo-lns#show users
    Line       User       Host(s)              Idle       Location
*  0 con 0     cisco      idle                 00:00:00

  Interface    User               Mode         Idle     Peer Address
  Vi4          demo@cisco.com     PPPoVPDN     00:00:01 10.5.110.245
  Vi5          demo@cisco.com     PPPoVPDN     00:00:01 10.5.110.244
```

2.4.3 Verify PPPoE Connectivity

Interface connecting to demo-pe1 is shutdown in all GMs.

Ping the Headquarters GM and other branch GM.

```
demo-gm1#ping 10.5.110.46 source vlan 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.110.46, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

demo-gm1#ping 10.5.110.245 source vlan 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.110.245, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Verify IP packets go via LNS.

```
demo-gm1#show ip route 10.5.110.46
Routing entry for 10.5.110.44/30
  Known via "eigrp 44", distance 90, metric 46228736, type internal
  Redistributing via eigrp 44
  Last update from 10.5.110.41 17:26:48 ago
  Routing Descriptor Blocks:
  * 10.5.110.41, from 10.5.110.41, 17:26:48 ago
      Route metric is 46228736, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 56 Kbit
      Reliability 255/255, minimum MTU 1492 bytes
      Loading 1/255, Hops 1
```

2.4.4 Verify GDOI Encrypted Traffic between Branches

2.4.4.1 GDOI Encrypted Traffic between Branches Using MPLS Core

```
demo-gm1#show crypto ipsec sa | incl encaps
```

```
    #pkts encaps: 14728, #pkts encrypt: 14728, #pkts digest: 14728
demo-gm1#ping 10.5.110.22 source vlan 10 rep 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.5.110.22, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/4 ms
demo-gm1#show crypto ipsec sa | incl encaps
    #pkts encaps: 14828, #pkts encrypt: 14828, #pkts digest: 14828
```

2.4.4.2 Verifying GDOI Encrypted Unicast Traffic between Branches and Headquarters Using PPPoE SP Path

```
demo-gm1(config)#int Dialer10
demo-gm1(config-if)#crypto
demo-gm1(config-if)#crypto map gdoi
demo-gm1(config-if)#exit

demo-gm2(config)#int Dialer10
demo-gm2(config-if)#crypto map gdoi
demo-gm2(config-if)#exit

demo-gm3(config-if)#int vlan 20
demo-gm3(config-if)#crypto map gdoi
demo-gm3(config-if)#exit
```

Verify GDOI encryption between the Branch1 and Headquarters:

```
demo-gm1#show crypto ipsec sa | incl encaps
    #pkts encaps: 241, #pkts encrypt: 241, #pkts digest: 241

demo-gm1#ping 10.5.110.46 source vlan 10 rep 100
Sending 100, 100-byte ICMP Echos to 10.5.110.46, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms

demo-gm1#show crypto ipsec sa | incl encaps
    #pkts encaps: 341, #pkts encrypt: 341, #pkts digest: 341
```

Verify GDOI encryption between the Branch1 and Branch2:

```
demo-gm1#show crypto ipsec sa | incl encaps
    #pkts encaps: 459, #pkts encrypt: 459, #pkts digest: 459

demo-gm1#ping 10.5.110.245 source vlan 10 rep 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.5.110.245, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/6/324 ms

demo-gm1#ping 10.5.110.245 source vlan 10 rep 100
*Feb 17 15:30:44 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO
from 10.5.show crypto ipsec sa | incl encaps
    #pkts encaps: 559, #pkts encrypt: 559, #pkts digest: 559
```

2.4.4.3 Verifying GDOI Encrypted Unicast Traffic between Branches and Headquarters with Large File Transfer

Large 55 Mb file is transferred from Headquarters and branch GM via PPPoE secondary SP network. GDOI encryption is verified.

```
demo-gm1#show crypto ipsec sa | incl encaps
    #pkts encaps: 471, #pkts encrypt: 471, #pkts digest: 471

demo-gm1#copy tftp: flash:
Address or name of remote host []? foo
Source filename []? /tftpboot/manis/c2800nm-adventerprisek9-mz.124-22.T

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 58246016 bytes]

58246016 bytes copied in 832.376 secs (69976 bytes/sec)
demo-gm1#show crypto ipsec sa | incl encaps
    #pkts encaps: 114420, #pkts encrypt: 114420, #pkts digest: 114420
```

2.4.4.4 Verifying Whether GM Receives Multicast Rekey

Following log messages in the GM verifies it.

```
*Feb 19 15:23:52: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO from
10.5.110.88 to 239.192.1.190 with seq # 101
*Feb 19 15:24:02: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO from
10.5.110.88 to 239.192.1.190 with seq # 102
*Feb 19 15:24:13: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO from
10.5.110.88 to 239.192.1.190 with seq # 103
demo-gm1#show crypto gdoi
GROUP INFORMATION
    Group Name               : GETVPN-DEMO
    Group Identity           : 1357924756
    Rekeys received          : 12
    IPSec SA Direction       : Both
    Active Group Server      : 10.5.110.88
    Group Server list        : 10.5.110.88
                               10.5.110.99
    GM Reregisters in        : 60 secs
    Rekey Received(hh:mm:ss) : 00:12:40
    Rekeys received
         Cumulative          : 12
         After registration  : 12
 ACL Downloaded From KS 10.5.110.88:
   access-list  deny udp any port = 848 any port = 848
   access-list  deny tcp any any port = 23
   access-list  deny tcp any port = 23 any
   access-list  deny esp any any
   access-list  deny tcp any port = 179 any
   access-list  deny udp any port = 500 any port = 500
   access-list  deny ospf any any
   access-list  deny eigrp any any
   access-list  deny igmp any any
   access-list  deny pim any any
   access-list  deny ip any 224.0.0.0 0.0.255.255
   access-list  deny udp any any port = 123
   access-list  deny udp any any port = 161
   access-list  deny udp any any port = 514
   access-list  permit ip any any
KEK POLICY:
    Rekey Transport Type      : Multicast
    Lifetime (secs)           : 2859
    Encrypt Algorithm         : AES
    Key Size                  : 128
    Sig Hash Algorithm        : HMAC_AUTH_SHA
    Sig Key Length (bits)     : 1024
TEK POLICY:
  Virtual-Access2:
  Dialer10:
    IPSec SA:
        sa direction:inbound
```

```
        spi: 0x19517674(424769140)
         transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (835)
        Anti-Replay(Time Based) : 5 sec interval
IPSec SA:
        sa direction:inbound
        spi: 0xE8510292(3897623186)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (835)
        Anti-Replay(Time Based) : 5 sec interval
    IPSec SA:
        sa direction:outbound
        spi: 0xE8510292(3897623186)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (835)
        Anti-Replay(Time Based) : 5 sec interval
```

2.5 Primary Network Failover Solution Test

2.5.1 Verify Primary Network Failover

Both Primary path and secondary SP network interfaces are in active state.

Apply the following ACL to Gi0/1 interface on demo-pe1 to simulate primary network failure:

```
ip access-list standard block-demo-gm1
 deny   10.5.110.17
demo-pe1(config)#int Gi0/1
demo-pe1(config-if)#ip access-group block-demo-gm1 in
```

Before ACL is applied, traffic flows through MPLS network.

```
demo-gm1#show crypto ipsec sa | begin GigabitEthernet0/0
interface: GigabitEthernet0/0
#pkts encaps: 45440, #pkts encrypt: 45440, #pkts digest: 45440

demo-gm1#show crypto ipsec sa | begin Dialer10
interface: Dialer10
#pkts encaps: 20092, #pkts encrypt: 20092, #pkts digest: 20092
```

Ping corporate address 10.5.110.9.

```
demo-gm1#ping 10.5.110.9 source vlan 10 rep 1000
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 4/4/8 ms

demo-gm1#show crypto ipsec sa | begin GigabitEthernet0/0
interface: GigabitEthernet0/0
#pkts encaps: 46440, #pkts encrypt: 46440, #pkts digest: 46440

demo-gm1#show crypto ipsec sa | begin Dialer10
interface: Dialer10
#pkts encaps: 20097, #pkts encrypt: 20097, #pkts digest: 20097
```

When ACL is applied, traffic flow switches to secondary SP network via PPPoE interface.

```
demo-gm1#show crypto ipsec sa | begin GigabitEthernet0/0
interface: GigabitEthernet0/0
#pkts encaps: 46527, #pkts encrypt: 46527, #pkts digest: 46527

demo-gm1#show crypto ipsec sa | begin Dialer10
interface: Dialer10
#pkts encaps: 20178, #pkts encrypt: 20178, #pkts digest: 20178

demo-gm1#ping 10.5.110.9 source vlan 10 rep 1000

demo-pe1(config)#int Gi0/1
demo-pe1(config-if)# ip access-group block-demo-gm1 in
demo-pe1(config-if)#

Ping result: Success rate is 99 percent (992/1000), round-trip min/avg/max = 4/4/28
ms
```

Traffic switched from MPLS network to PPPoE secondary SP network.

```
demo-gm1#show crypto ipsec sa | begin GigabitEthernet0/0
interface: GigabitEthernet0/0
#pkts encaps: 47339, #pkts encrypt: 47339, #pkts digest: 47339

demo-gm1#show crypto ipsec sa | begin Dialer10
interface: Dialer10
#pkts encaps: 20382, #pkts encrypt: 20382, #pkts digest: 20382
```

2.5.2 Verify Primary Network Recovery and Traffic Flow Switch to Primary Network

When ACL is removed, traffic flow switches to primary MPLS SP network.

```
demo-gm1#show crypto ipsec sa | begin GigabitEthernet0/0
interface: GigabitEthernet0/0
#pkts encaps: 48656, #pkts encrypt: 48656, #pkts digest: 48656

demo-gm1#show crypto ipsec sa | begin Dialer10
interface: Dialer10
#pkts encaps: 23007, #pkts encrypt: 23007, #pkts digest: 23007

demo-gm1#ping 10.5.110.9 source vlan 10 rep 10000

demo-pe1(config)#int Gi0/1
demo-pe1(config-if)#no ip access-group block-demo-gm1 in
demo-pe1(config-if)#

demo-gm1#show crypto ipsec sa | begin GigabitEthernet0/0
interface: GigabitEthernet0/0
#pkts encaps: 55579, #pkts encrypt: 55579, #pkts digest: 55579

demo-gm1#show crypto ipsec sa | begin Dialer10
```

```
interface: Dialer10
#pkts encaps: 26115, #pkts encrypt: 26115, #pkts digest: 26115
```

2.6 Reference Configuration of Solution Test Setup

Following sections lists configuration listing of the routers used in the Solution Test setup.

2.6.1 Reference Configuration of demo-pe1

Following is running-config of demo-pe1:

```
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname demo-pe1
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip cef
ip multicast-routing
ip igmp ssm-map enable
no ipv6 cef
username cisco password lab
!
interface GigabitEthernet0/1
 description connected to demo-gm1
 ip address 10.5.110.18 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/2
 description Connected to demo-gm2
 ip address 10.5.110.21 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/3
 description Connected to demo-gm3
 ip address 10.5.110.29 255.255.255.252
 ip pim sparse-mode
!
router eigrp 44
 network 10.5.110.16 0.0.0.3
 network 10.5.110.20 0.0.0.3
 network 10.5.110.28 0.0.0.3
 auto-summary
!
ip pim ssm range 1
!
access-list 1 permit 239.192.0.0 0.0.255.255
!
line con 0
```

```
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
 login
!
end
```

2.6.2 Reference Configuration of demo-gm1

Following is running-config of demo-gm1:

```
!
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname demo-gm1
!
aaa new-model
!
aaa authentication ppp default local
!
aaa session-id common
clock timezone pst -8
clock summer-time pst recurring
!
ip cef
!
ip dhcp pool demo
   network 10.5.110.200 255.255.255.248
   domain-name cisco.com
   dns-server 171.68.226.120
   default-router 10.5.110.201
   netbios-name-server 171.68.235.228
   option 150 ip 171.70.112.211
!
ip domain name cisco.com
ip multicast-routing
ip dhcp-server 10.5.110.201
ip igmp ssm-map enable
no ipv6 cef
!
username demo password lab
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key dGvPnPsK address 0.0.0.0 0.0.0.0
```

```
!
crypto gdoi group GETVPN-DEMO
 identity number 1357924756
 server address ipv4 10.5.110.88
 server address ipv4 10.5.110.99
!
crypto map demo-gdoi local-address Vlan10
crypto map demo-gdoi 1 gdoi
 set group GETVPN-DEMO
 match address no-encryption-acl
!
bba-group pppoe global
!
interface GigabitEthernet0/0
 description Connected to demo-pe1
 ip address 10.5.110.17 255.255.255.252
 ip pim sparse-mode
crypto map demo-gdoi
!
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet1/0
 description connected to demo-lac
 no switchport
 no ip address
 ip pim sparse-mode
 ip tcp adjust-mss 1452
 pppoe enable group global
 pppoe-client dial-pool-number 10
!
interface Vlan10
 ip address 10.5.110.201 255.255.255.248
 ip pim sparse-mode
 ip igmp join-group 239.192.1.190 source 10.5.110.88
 ip igmp join-group 239.192.1.190 source 10.5.110.99
no autostate
!
interface Dialer10
 ip address negotiated
 ip mtu 1492
 ip pim sparse-mode
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip mroute-cache
 dialer pool 10
 ppp authentication pap
 ppp pap sent-username demo@cisco.com password lab
```

```
 crypto map demo-gdoi
!
router eigrp 44
 network 10.5.110.12 0.0.0.3
 network 10.5.110.16 0.0.0.3
 network 10.5.110.200 0.0.0.7
 network 10.5.110.240 0.0.0.7
 no auto-summary
!
ip pim ssm range 1
ip nat inside source list 10 interface Dialer10 overload
!
ip access-list extended no-encryption-acl
 deny   udp 10.5.110.0 0.0.0.255 eq 848 10.5.110.0 0.0.0.255 eq 848
 deny   ip any host 239.192.1.190
!
access-list 1 permit 239.192.0.0 0.0.255.255
access-list 10 permit 10.5.110.200 0.0.0.7
dialer-list 10 protocol ip list 10
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
end
```

2.6.3 Reference Configuration of demo-gm2

Following is running-config of demo-gm2:

```
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname demo-gm2
!
enable secret lab
!
aaa new-model
!
aaa authentication ppp default local
!
aaa session-id common
clock timezone PST -8
clock summer-time PDT recurring
!
ip cef
!
ip dhcp pool demo
   network 10.5.110.208 255.255.255.248
   default-router 10.5.110.209
!
ip domain name cisco.com
ip multicast-routing
ip igmp ssm-map enable
no ipv6 cef
!
username demo password lab
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key dGvPnPsK address 0.0.0.0 0.0.0.0
!
crypto gdoi group GETVPN-DEMO
 identity number 1357924756
 server address ipv4 10.5.110.88
 server address ipv4 10.5.110.99
!
crypto map demo-gdoi  local-address Vlan10
crypto map demo-gdoi 1 gdoi
 set group GETVPN-DEMO
 match address no-encryption-acl
!
bba-group pppoe global
!
```

```
interface GigabitEthernet0/0
 description connected to demo-gm1
 no ip dhcp client request tftp-server-address
 ip address 10.5.110.22 255.255.255.252
 ip pim sparse-mode
 crypto map demo-gdoi
!
interface GigabitEthernet0/1
 description Connected to demo-ks2
 ip address 10.5.110.25 255.255.255.252
 ip pim sparse-mode
!
interface FastEthernet1/0
 description connected to demo-lac
 no switchport
 no ip address
 ip pim sparse-mode
 ip tcp adjust-mss 1452
 pppoe enable group global
 pppoe-client dial-pool-number 10
!
interface Vlan10
 ip address 10.5.110.209 255.255.255.248
 ip pim sparse-mode
 ip nat inside
 ip virtual-reassembly
 ip tcp adjust-mss 1452
 ip igmp join-group 239.192.1.190 source 10.5.110.88
 ip igmp join-group 239.192.1.190 source 10.5.110.99
 no ip mroute-cache
 no autostate
!
interface Dialer10
 ip address negotiated
 ip mtu 1492
 ip pim sparse-mode
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip mroute-cache
 dialer pool 10
 ppp authentication pap
 ppp pap sent-username demo@cisco.com password lab
 crypto map demo-gdoi
!
router eigrp 44
 network 10.5.110.20 0.0.0.3
 network 10.5.110.24 0.0.0.3
 network 10.5.110.208 0.0.0.7
 network 10.5.110.240 0.0.0.7
```

```
 no auto-summary
!
ip pim ssm range 1
ip nat inside source list 10 interface Dialer10 overload
!
ip access-list extended no-encryption-acl
 deny   udp 10.5.110.0 0.0.0.255 eq 848 10.5.110.0 0.0.0.255 eq 848
 deny   ip any host 239.192.1.190
!
access-list 1 permit 239.192.0.0 0.0.255.255
access-list 10 permit 10.5.110.208 0.0.0.7
dialer-list 10 protocol ip list 10
!
line con 0
line aux 0
line vty 0 4
 password lab
!
end
```

2.6.4 Reference Configuration of demo-gm3

Following is running-config of demo-gm3:

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname demo-gm3
!
enable secret lab
!
ip dhcp pool demo
   network 10.5.110.216 255.255.255.248
   default-router 10.5.110.217
!
ip cef
ip domain name cisco.com
ip multicast-routing
ip igmp ssm-map enable
no ipv6 cef
!
username demo password lab
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key dGvPnPsK address 0.0.0.0 0.0.0.0
!
crypto gdoi group GETVPN-DEMO
```

```
 identity number 1357924756
 server address ipv4 10.5.110.88
 server address ipv4 10.5.110.99
!
crypto map demo-gdoi local-address Vlan10
crypto map demo-gdoi 1 gdoi
 set group GETVPN-DEMO
 match address no-encryption-acl
!
interface FastEthernet0/0
 description Connected to demo-pe1
 ip address 10.5.110.30 255.255.255.252
 ip pim sparse-mode
crypto map demo-gdoi
!
interface FastEthernet0/1
 ip address 10.5.110.10 255.255.255.252
!
interface FastEthernet0/1/0
 switchport access vlan 10
!
interface FastEthernet0/1/7
 description Connected to demo-ks1
 switchport access vlan 30
!
interface FastEthernet0/1/8
 switchport access vlan 20
!
interface Vlan10
 ip address 10.5.110.217 255.255.255.248
 ip pim sparse-mode
 ip igmp join-group 239.192.1.190 source 10.5.110.88
 ip igmp join-group 239.192.1.190 source 10.5.110.99
 no autostate
!
interface Vlan20
 ip address 10.5.110.46 255.255.255.252
 ip pim sparse-mode
 no autostate
 crypto map demo-gdoi
!
interface Vlan30
 description Connected to demo-ks1
 ip address 10.5.110.14 255.255.255.252
 ip pim sparse-mode
 no autostate
!
router eigrp 44
 redistribute static
 network 10.5.110.8 0.0.0.3
```

```
 network 10.5.110.12 0.0.0.3
 network 10.5.110.28 0.0.0.3
 network 10.5.110.44 0.0.0.3
 network 10.5.110.216 0.0.0.7
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.5.110.9
!
ip pim ssm range 1
!
ip access-list extended no-encryption-acl
 deny   udp 10.5.110.0 0.0.0.255 eq 848 10.5.110.0 0.0.0.255 eq 848
 deny   ip any host 239.192.1.190
!
access-list 1 permit 239.192.0.0 0.0.255.255
!
line con 0
line aux 0
line vty 0 4
 password 7 141B1309
 login
!
end
```

2.6.5 Reference Configuration of demo-ks1

Following is running-config of demo-ks1:

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname demo-ks1
!
enable secret lab
!
ip cef
!
ip domain name cisco.com
ip multicast-routing
no ipv6 cef
username cisco password 0 getvpn-demo
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key dGvPnPsK address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 15 periodic
!
crypto ipsec transform-set aes128 esp-aes esp-sha-hmac
```

```
!
crypto ipsec profile getvpn-profile
 set security-association lifetime seconds 900
 set transform-set aes128
!
crypto gdoi group GETVPN-DEMO
 identity number 1357924756
 server local
  rekey algorithm aes 128
  rekey address ipv4 dgvpn-rekey-multicast-group
  rekey lifetime seconds 28800
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa
  sa ipsec 1
   profile getvpn-profile
   match address ipv4 sa-acl
   replay time window-size 5
  address ipv4 10.5.110.88
  redundancy
   local priority 23
   peer address ipv4 10.5.110.99
!
interface Loopback0
 ip address 10.5.110.88 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet0/1
 description Connected to demo-gm1
 ip address 10.5.110.13 255.255.255.252
 ip pim sparse-mode
!
router eigrp 44
 network 10.5.110.12 0.0.0.3
 network 10.5.110.88 0.0.0.0
 no auto-summary
!
ip pim ssm range 1
!
ip access-list extended dgvpn-rekey-multicast-group
 permit ip any host 239.192.1.190
ip access-list extended sa-acl
 deny   udp 10.5.110.0 0.0.0.255 eq 848 10.5.110.0 0.0.0.255 eq 848
 deny   tcp any any eq telnet
 deny   tcp any eq telnet any
 deny   esp any any
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   udp any eq isakmp any eq isakmp
 deny   ospf any any
 deny   eigrp any any
```

```
 deny   igmp any any
 deny   pim any any
 deny   ip any 224.0.0.0 0.0.255.255
 deny   udp any any eq ntp
 deny   udp any any eq snmp
 deny   udp any any eq syslog
 permit ip any any
!
logging alarm informational
access-list 1 permit 239.192.0.0 0.0.255.255
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
 login
!
end
```

2.6.6 Reference Configuration of demo-ks2

Following is running-config of demo-ks2:

```
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname demo-ks2
!
ip cef
!
ip domain name cisco.com
ip multicast-routing
username cisco password 0 getvpn-demo
archive
 log config
  hidekeys
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key dGvPnPsK address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 15 periodic
!
crypto ipsec transform-set aes128 esp-aes esp-sha-hmac
!
crypto ipsec profile getvpn-profile
```

```
 set security-association lifetime seconds 900
 set transform-set aes128
!
crypto gdoi group GETVPN-DEMO
 identity number 1357924756
 server local
  rekey algorithm aes 128
  rekey address ipv4 dgvpn-rekey-multicast-group
  rekey lifetime seconds 28800
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa
  sa ipsec 1
   profile getvpn-profile
   match address ipv4 sa-acl
   replay time window-size 5
  address ipv4 10.5.110.99
  redundancy
   local priority 22
   peer address ipv4 10.5.110.88
!
interface Loopback0
 ip address 10.5.110.99 255.255.255.255
 ip mtu 1492
 ip pim sparse-mode
!
interface GigabitEthernet0/1
 description Connected to demo-gm1
 ip address 10.5.110.26 255.255.255.252
 ip pim sparse-mode
!
router eigrp 44
 network 10.5.110.24 0.0.0.3
 network 10.5.110.99 0.0.0.0
 no auto-summary
!
ip pim ssm range 1
!
ip access-list extended dgvpn-rekey-multicast-group
 permit ip any host 239.192.1.190
ip access-list extended sa-acl
 deny   udp 10.5.110.0 0.0.0.255 eq 848 10.5.110.0 0.0.0.255 eq 848
 deny   tcp any any eq telnet
 deny   tcp any eq telnet any
 deny   esp any any
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   udp any eq isakmp any eq isakmp
 deny   ospf any any
 deny   eigrp any any
 deny   igmp any any
```

```
 deny   pim any any
 deny   ip any 224.0.0.0 0.0.255.255
 deny   udp any any eq ntp
 deny   udp any any eq snmp
 deny   udp any any eq syslog
 permit ip any any
!
access-list 1 permit 239.192.0.0 0.0.255.255
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```

2.6.7 Reference Configuration of demo-lac

Following is running-config of demo-lac:

```
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname demo-lac
!
enable password lab
!
aaa new-model
!
aaa authentication ppp default local
!
aaa session-id common
clock timezone pst -8
clock summer-time pst recurring
ip cef
!
ip multicast-routing
ip igmp ssm-map enable
no ipv6 cef
!
vpdn enable
!
vpdn-group demo-getvpn-pppoe
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.5.110.41
```

```
 local name demo-lac
 l2tp tunnel password lab
username demo password lab
!
bba-group pppoe demo-getvpn-pppoe
 virtual-template 11
 sessions auto cleanup
!
interface GigabitEthernet0/0
 description connected to demo-gm1
 ip address 10.5.110.34 255.255.255.252
 ip pim sparse-mode
 pppoe enable group demo-getvpn-pppoe
!
interface GigabitEthernet0/1
 description connected to demo-gm2
 ip address 10.5.110.37 255.255.255.252
 ip pim sparse-mode
 pppoe enable group demo-getvpn-pppoe
!
interface GigabitEthernet0/2
 description connected to LNS
 ip address 10.5.110.42 255.255.255.252
 ip pim sparse-mode
!
interface Virtual-Template11
 no ip address
 ip mtu 1492
 no ip route-cache cef
 ppp authentication pap
 ppp pap sent-username demo password lab
!
router eigrp 44
 network 10.5.110.32 0.0.0.3
 network 10.5.110.36 0.0.0.3
 network 10.5.110.40 0.0.0.3
 network 10.5.110.240 0.0.0.7
 no auto-summary
!
ip pim ssm range 1
!
access-list 1 permit 239.192.0.0 0.0.255.255
!
line con 0
 exec-timeout 0 0
 transport output all
 stopbits 1
line aux 0
stopbits 1
line vty 0 4
```

```
 password lab
!
end
```

2.6.8 Reference Configuration of demo-lns

Following is running-config of demo-lns:

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname demo-lns
!
enable secret lab
!
aaa new-model
!
aaa authentication ppp default local
!
aaa session-id common
clock timezone pst -8
clock summer-time pst recurring
!
ip cef
!
ip domain name cisco.com
ip multicast-routing
ip igmp ssm-map enable
no ipv6 cef
!
vpdn enable
!
vpdn-group demo-getvpn-pppoe
 accept-dialin
  protocol l2tp
  virtual-template 10
 terminate-from hostname demo-lac
 local name demo-lns
 l2tp tunnel password lab
!
username demo@cisco.com password lab
username demo password lab
!
interface GigabitEthernet0/0
 ip address 10.5.110.41 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/1
 ip address 10.5.110.45 255.255.255.252
 ip pim sparse-mode
```

```
!
interface Virtual-Template10
 ip unnumbered GigabitEthernet0/0
 ip mtu 1492
 ip pim sparse-mode
 no ip route-cache cef
 peer default ip address pool l2tp-pool
 ppp authentication pap
 ppp pap sent-username demo password 7 060A0E23
!
router eigrp 44
 network 10.5.110.40 0.0.0.3
 network 10.5.110.44 0.0.0.3
 network 10.5.110.240 0.0.0.7
 no auto-summary
!
ip local pool l2tp-pool 10.5.110.242 10.5.110.246
!
ip pim ssm range 1
!
access-list 1 permit 239.192.0.0 0.0.255.255
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end
```

3. Using GDOI Encryption in DMVPN Secondary SP Network

3.1 Objective

Following are objectives of the solution test.

- **Test GDOI encryption of traffic via DMVPN Tunnel network path.**
- **Test failover of primary SP network.** When primary SP network fails, traffic will flow through the secondary SP network. When the primary SP network is restored, traffic will switch back to primary SP network from the secondary SP network.

3.2 Solution Test Topology

GETVPN solution test setup consists of three GMs (Group Members) and two KSs (Key Servers). “demo-pe1” simulates the MPLS primary SP network.

Key servers are connected to both Primary and Secondary SP networks.

3.2.1 DMVPN Secondary Path Setup

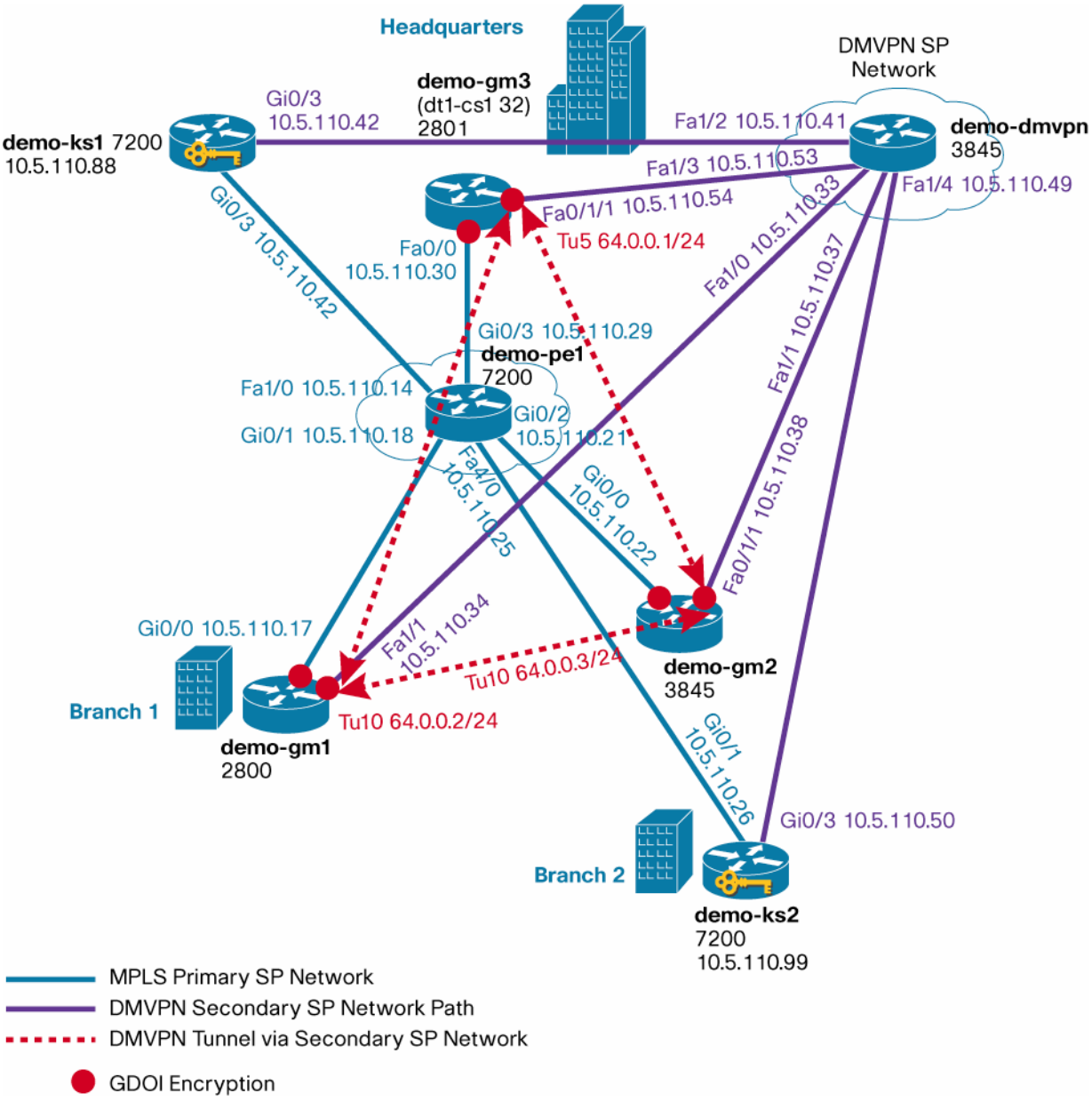
Solution test setup consists of two DMVPN spoke routers demo-gm1 and demo-gm2 located in branches and one DMVPN hub router demo-gm3 located in the head quarters. “demo-dmvpn” simulates the IP VPN network. 3845 platform routers running 12.4(22)T IOS image are used.

For enterprise IPSec VPNs that traverse the public Internet, Group Encrypted Transport enhances Dynamic Multipoint VPN (DMVPN) and GRE-based site-to-site VPNs by providing manageable, highly scalable network meshing cost-effectively by using the group shared key. Hub-and-Spoke and Spoke-to-Spoke DMVPN (mGRE) tunnels established with IPSec protection. GDOI encryption is applied to the Tunnel Interface.

EIGRP routing protocol is used for DMVPN. Provider equipment uses BGP routing protocol.

GDOI encryption is done on the customer network side in the GM routers. Traffic flowing through the interface connected to primary SP network and the interface connected to the secondary service provider network are GDOI encrypted.

Figure 2. DMVPN Secondary SP Network with GDOI Encryption in the GMs



3.3 DMVPN Secondary SP Network Configuration

Following sections provide DMVPN configuration commands needed for provisioning DMVPN secondary SP network with GDOI encryption.

3.3.1 Configuration of GM in Branch 1 (demo-gm1)

Following includes DMVPN with GDOI encryption configuration in demo-gm1:

```
!
hostname demo-gm1
!
ip dhcp pool demo
   network 10.5.110.200 255.255.255.248  ! Private local network
   default-router 10.5.110.201
```

```
ip multicast-routing
ip igmp ssm-map enable
! GDOI IKE policy
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
! Pre-shared keys
crypto isakmp key dGvPnPsK address 10.5.110.88
crypto isakmp key dGvPnPsK address 10.5.110.99
! GM GDOI Group configuration
crypto gdoi group GETVPN-DEMO
 identity number 1357924756
 server address ipv4 10.5.110.88
 server address ipv4 10.5.110.99
! IKE connection is registered via Vlan 10
crypto map demo-gdoi local-address Vlan10
! GDOI crypto map configuration
crypto map demo-gdoi 1 gdoi
 set group GETVPN-DEMO
! DMVPN tunnel with GDOI encryption
interface Tunnel10
  bandwidth 2000
  ip address 64.0.0.2 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip pim sparse-dense-mode
  ip nhrp map multicast 10.5.110.54
  ip nhrp map 64.0.0.1 10.5.110.54
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 64.0.0.1
  ip nhrp shortcut
  ip nhrp redirect
  ip tcp adjust-mss 1360
  delay 2000
  qos pre-classify
  tunnel source FastEthernet1/1
  tunnel mode gre multipoint
  tunnel key 100000
  crypto map demo-gdoi  ! GDOI encryption applied on the Tunnel IF
!
interface GigabitEthernet0/0
 description Connected to demo-pe1
 ip address 10.5.110.17 255.255.255.252
 ip flow ingress
 ip pim sparse-mode
 duplex auto
 speed auto
 crypto map demo-gdoi ! GDOI encryption applies
```

```
!
 interface FastEthernet1/1
   description connected to demo_dmvpn
   ip address 10.5.110.34 255.255.255.252
   ip pim sparse-mode
!
interface Vlan10
 ip address 10.5.110.201 255.255.255.248
 ip pim sparse-mode
 ip igmp join-group 239.192.1.190 source 10.5.110.88
 ip igmp join-group 239.192.1.190 source 10.5.110.99
 no autostate
!
 router eigrp 44
   network 10.5.110.200 0.0.0.7  ! private local network
   network 64.0.0.0 0.0.0.255    ! Secondary SP DMVPN Tunnel network
   no auto-summary
!
router bgp 200
   no synchronization
   bgp log-neighbor-changes
   network 10.5.110.16 mask 255.255.255.252  ! netowork connected to primary SP
   network 10.5.110.200 mask 255.255.255.248 ! private local network
   neighbor 10.5.110.18 remote-as 100
   neighbor 10.5.110.33 remote-as 900
   no auto-summary
!
 ip route 0.0.0.0 0.0.0.0 10.5.110.33      ! Default route for DMVPN
!
ip pim ssm range 1
!
access-list 1 permit 239.192.0.0 0.0.255.255 ! ACL for SSM
```

3.3.2 Configuration of GM in Branch 2 (demo-gm2)

Following includes DMVPN with GDOI encryption configuration in demo-gm2:

```
!
hostname demo-gm2
!
ip dhcp pool demo
   network 10.5.110.208 255.255.255.248    ! private local network
   default-router 10.5.110.209
!
ip multicast-routing
ip igmp ssm-map enable
! IKE policy for GDOI
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
```

```
! pre-shared keys
! For IPSec preshared keys you need to add one for each spoke or hub
! But for GDOI, it is enough to add entries for KS IKE keys
crypto isakmp key dGvPnPsK address 10.5.110.88
crypto isakmp key dGvPnPsK address 10.5.110.99
! GM GDOI group configuration
crypto gdoi group GETVPN-DEMO
 identity number 1357924756
 server address ipv4 10.5.110.88
 server address ipv4 10.5.110.99
! IKE connection is registered via Vlan 10
crypto map demo-gdoi local-address Vlan10
! GDOI crypto map
crypto map demo-gdoi 1 gdoi
 set group GETVPN-DEMO
! DMVPN tunnel with GDOI encryption
interface Tunnel10
 bandwidth 2000
 ip address 64.0.0.3 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip pim sparse-dense-mode
 ip nhrp map multicast 10.5.110.54
 ip nhrp map 64.0.0.1 10.5.110.54
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 64.0.0.1
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 2000
 qos pre-classify
 tunnel source Vlan3
 tunnel mode gre multipoint
 tunnel key 100000
 crypto map demo-gdoi     ! GDOI encryption on DMVPN tunnel
!
interface GigabitEthernet0/0
 description connected to demo-pe1
 ip address 10.5.110.22 255.255.255.252
 ip pim sparse-mode
 crypto map demo-gdoi    ! GDOI encryption on interface connected to primary SP
!
interface FastEthernet0/1/1
 description conneted to demo_dmvpn
 switchport access vlan 3
!
interface Vlan3
 description conneted to demo_dmvpn
 ip address 10.5.110.38 255.255.255.252
```

```
 ip pim sparse-mode
!
interface Vlan10
 ip address 10.5.110.209 255.255.255.248
 ip pim sparse-mode
 ip igmp join-group 239.192.1.190 source 10.5.110.88
 ip igmp join-group 239.192.1.190 source 10.5.110.99
 no autostate
!
router eigrp 44
  network 10.5.110.208 0.0.0.7 ! private local network
  network 64.0.0.0 0.0.0.255   ! Secondary SP DMVPN Tunnel network
  no auto-summary
!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 network 10.5.110.20 mask 255.255.255.252  ! Primary SP network
 network 10.5.110.208 mask 255.255.255.252 ! private local network
 neighbor 10.5.110.21 remote-as 100
 neighbor 10.5.110.37 remote-as 900
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.5.110.37    ! Default route for DMVPN
!
ip pim ssm range 1
access-list 1 permit 239.192.0.0 0.0.255.255  ! ACL for SSM
```

3.3.3 Configuration of GM in Headquarters (demo-gm3)

Following lists DMVPN with GDOI encryption configuration in demo-gm3:

```
!
hostname demo-gm3
!
ip dhcp pool demo
   network 10.5.110.216 255.255.255.248   ! Private local network
   default-router 10.5.110.217
!
ip multicast-routing
ip igmp ssm-map enable
! IKE policy for GETVPN
 crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!  preshared keys
crypto isakmp key dGvPnPsK address 10.5.110.88
crypto isakmp key dGvPnPsK address 10.5.110.99
! GM GDOI group configuration
crypto gdoi group GETVPN-DEMO
```

```
 identity number 1357924756
 server address ipv4 10.5.110.88
 server address ipv4 10.5.110.99
! IKE connection is registered via Vlan 10
crypto map demo-gdoi local-address Vlan10
! GDOI crypto map
crypto map demo-gdoi 1 gdoi
 set group GETVPN-DEMO
! DMVPN Tunnel in Headquarters
 interface Tunnel5
  bandwidth 2000
  ip address 64.0.0.1 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip pim nbma-mode
  ip pim sparse-dense-mode
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp redirect
  ip tcp adjust-mss 1360
  no ip split-horizon eigrp 44
  delay 2000
  qos pre-classify
  tunnel source Vlan5
  tunnel mode gre multipoint
  tunnel key 100000
  crypto map demo-gdoi   ! GDOI crypto map applied
!
interface FastEthernet0/0
 description Connected to demo-pe1
 ip address 10.5.110.30 255.255.255.252
 ip pim sparse-mode
 crypto map demo-gdoi  ! GDOI crypto map applied to IF connected to primary network
!
interface FastEthernet0/1/1
 description conneted to demo_dmvpn
 switchport access vlan 5
!
 interface Vlan5
  description conneted to demo_dmvpn
  ip address 10.5.110.54 255.255.255.252
  ip pim sparse-mode
!
 interface Vlan10
  ip address 10.5.110.217 255.255.255.248
  ip pim sparse-mode
  ip igmp join-group 239.192.1.190 source 10.5.110.88
  ip igmp join-group 239.192.1.190 source 10.5.110.99
  ip igmp join-group 239.255.255.249 source 10.5.110.211
  ip igmp join-group 239.255.255.250 source 10.5.110.211
```

```
  no autostate
!
router eigrp 44
 redistribute static
 network 10.5.110.216 0.0.0.7  ! private local network
 network 64.0.0.0 0.0.0.255    ! Seondary SP DMVPN Tunnel network
 no auto-summary
!
router bgp 400
 no synchronization
 bgp log-neighbor-changes
 network 10.5.110.28 mask 255.255.255.252 ! network connected to primary SP
 network 10.5.110.216 mask 255.255.255.252 ! private local network
 neighbor 10.5.110.29 remote-as 100
 neighbor 10.5.110.53 remote-as 900
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.5.110.9  ! Default route to corporate network
ip route 10.5.110.32 255.255.255.252 10.5.110.53 ! Default route to Branch 1
ip route 10.5.110.36 255.255.255.252 10.5.110.53 ! Default route to Branch 2
!
ip pim ssm range 1
!
access-list 1 permit 239.192.0.0 0.0.255.255
```

3.3.4 Configuration of Primary KS (demo-ks1)

Following lists configuration in demo-ks1:

```
hostname demo-ks1
!
ip multicast-routing
! IKE Policy
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
! preshared keys
crypto isakmp key dGvPnPsK address 10.5.110.201
crypto isakmp key dGvPnPsK address 10.5.110.209
crypto isakmp key dGvPnPsK address 10.5.110.217
! Keepalive for co-op KS
crypto isakmp keepalive 15 periodic
!
crypto ipsec transform-set aes128 esp-aes esp-sha-hmac
!  IPSEC profile
crypto ipsec profile getvpn-profile
 set security-association lifetime seconds 900  ! TEK lifetime
 set transform-set aes128
!   GDOI group configuration
crypto gdoi group GETVPN-DEMO
```

```
 identity number 1357924756
 server local
  rekey algorithm aes 128
  rekey address ipv4 dgvpn-rekey-multicast-group
  rekey lifetime seconds 28800                    ! KEK lifetime
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa
  sa ipsec 1
   profile getvpn-profile
   match address ipv4 sa-acl
   replay time window-size 5
   address ipv4 10.5.110.88
  redundancy   ! Co-op KS configuration
   local priority 20
   peer address ipv4 10.5.110.99
!
interface Loopback0
 ip address 10.5.110.88 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet0/1
 description Connected to demo-pe1 (primary SP network)
 ip address 10.5.110.13 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/3
 description conneted to demo_dmvpn (secondary SP network)
 ip address 10.5.110.42 255.255.255.252
 ip pim sparse-mode
!
router bgp 800
  no synchronization
  bgp log-neighbor-changes
  network 10.5.110.12 mask 255.255.255.252
  network 10.5.110.40 mask 255.255.255.252
  network 10.5.110.88 mask 255.255.255.255
  neighbor 10.5.110.14 remote-as 100
  neighbor 10.5.110.41 remote-as 900
  no auto-summary
!
ip pim ssm range 1
! ACL for rekey multicast group
ip access-list extended dgvpn-rekey-multicast-group
 permit ip any host 239.192.1.190
! SA ACL
ip access-list extended sa-acl
 deny   udp any eq 848 any eq 848
 deny   tcp any any eq telnet
 deny   tcp any eq telnet any
 deny   esp any any
```

```
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   udp any eq isakmp any eq isakmp
 deny   ospf any any
 deny   eigrp any any
 deny   icmp any any
 deny   igmp any any
 deny   pim any any
 deny   ip any 224.0.0.0 0.0.255.255
 deny   udp any any eq ntp
 deny   udp any any eq snmp
 deny   udp any any eq syslog
 permit ip any any
!
access-list 1 permit 239.192.0.0 0.0.255.255  ! SSM ACL
```

3.3.5 Configuration of Secondary KS (demo-ks2)

Following lists configuration in demo-ks2:

```
hostname  demo-ks2
!
ip multicast-routing
! IKE policy
crypto isakmp policy 6
 encr 3des
 authentication pre-share
 group 2
 ! preshared keys
crypto isakmp key dGvPnPsK address 10.5.110.201
crypto isakmp key dGvPnPsK address 10.5.110.209
crypto isakmp key dGvPnPsK address 10.5.110.217
! Keepalive for co-op KS
crypto isakmp keepalive 15 periodic
!
crypto ipsec transform-set aes128 esp-aes esp-sha-hmac
!  IPSEC profile
crypto ipsec profile getvpn-profile
 set security-association lifetime seconds 900  ! TEK lifetime
 set transform-set aes128
!   GDOI group configuration
crypto gdoi group GETVPN-DEMO
 identity number 1357924756
 server local
  rekey algorithm aes 128
  rekey address ipv4 dgvpn-rekey-multicast-group
  rekey lifetime seconds 28800                  ! KEK lifetime
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa
  sa ipsec 1
   profile getvpn-profile
```

```
   match address ipv4 sa-acl
   replay time window-size 5
   address ipv4 10.5.110.99
  redundancy   ! Co-op KS configuration
   local priority 20
   peer address ipv4 10.5.110.88
!
interface Loopback0
 ip address 10.5.110.99 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet0/1
 description Connected to demo-pe1 (primary SP network)
 ip address 10.5.110.26 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/3
 description conneted to demo_dmvpn (secondary SP network)
 ip address 10.5.110.50 255.255.255.252
 ip pim sparse-mode
!
router bgp 1000
 no synchronization
 bgp log-neighbor-changes
 network 10.5.110.24 mask 255.255.255.252
 network 10.5.110.48 mask 255.255.255.252
 network 10.5.110.99 mask 255.255.255.255
 neighbor 10.5.110.25 remote-as 100
 neighbor 10.5.110.49 remote-as 900
 no auto-summary
!
ip pim ssm range 1
! ACL for rekey multicast group
ip access-list extended dgvpn-rekey-multicast-group
 permit ip any host 239.192.1.190
! SA ACL
ip access-list extended sa-acl
 deny   udp any eq 848 any eq 848
 deny   tcp any any eq telnet
 deny   tcp any eq telnet any
 deny   esp any any
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   udp any eq isakmp any eq isakmp
 deny   ospf any any
 deny   eigrp any any
 deny   icmp any any
 deny   igmp any any
 deny   pim any any
 deny   ip any 224.0.0.0 0.0.255.255
```

```
 deny   udp any any eq ntp
 deny   udp any any eq snmp
 deny   udp any any eq syslog
 permit ip any any
!
access-list 1 permit 239.192.0.0 0.0.255.255  ! SSM ACL
```

3.3.5 Configuration of demo-pe1

Demo-pe1 simulates the MPLS network. Following lists configuration in demo-pe1:

```
!
hostname demo-pe1
!
ip multicast-routing
!
interface GigabitEthernet0/1
 description connected to demo-gm1
 ip address 10.5.110.18 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/2
 description Connected to demo-gm2
 ip address 10.5.110.21 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/3
 description Connected to demo-gm3
 ip address 10.5.110.29 255.255.255.252
 ip pim sparse-mode
!
interface FastEthernet1/0
 description Connected to demo-ks1
 ip address 10.5.110.14 255.255.255.252
 ip pim sparse-mode
!
 interface FastEthernet4/0
 description Connected to demo-ks2
 ip address 10.5.110.25 255.255.255.252
 ip pim sparse-mode
!
router bgp 100
   no synchronization
   bgp log-neighbor-changes
   network 10.5.110.12 mask 255.255.255.252
   network 10.5.110.16 mask 255.255.255.252
   network 10.5.110.20 mask 255.255.255.252
   network 10.5.110.24 mask 255.255.255.252
   network 10.5.110.28 mask 255.255.255.252
   neighbor 10.5.110.13 remote-as 800
   neighbor 10.5.110.17 remote-as 200
```

```
   neighbor 10.5.110.22 remote-as 300
   neighbor 10.5.110.26 remote-as 900
   neighbor 10.5.110.30 remote-as 400
   no auto-summary
```

3.3.6 Configuration of demo-dmvpn

Demo-dmvpn simulates the VPN network. Following lists configuration in demo-dmvpn:

```
!
hostname demo_dmvpn
!
ip multicast-routing
!
interface FastEthernet1/0
 description connected to GM1
 ip address 10.5.110.33 255.255.255.252
 ip pim sparse-mode
!
interface FastEthernet1/1
 description connected to GM2
 ip address 10.5.110.37 255.255.255.252
 ip pim sparse-mode
!
interface FastEthernet1/2
 description connected to KS1
 ip address 10.5.110.41 255.255.255.252
 ip pim sparse-mode
!
interface FastEthernet1/3
 description connected to GM3
 ip address 10.5.110.53 255.255.255.252
 ip pim sparse-mode
!
interface FastEthernet1/4
description connected to KS2
 ip address 10.5.110.49 255.255.255.252
 ip pim sparse-mode
!
router bgp 900
 no synchronization
 bgp log-neighbor-changes
 network 10.5.110.32 mask 255.255.255.252
 network 10.5.110.36 mask 255.255.255.252
 network 10.5.110.40 mask 255.255.255.252
 network 10.5.110.48 mask 255.255.255.252
 network 10.5.110.52 mask 255.255.255.252
 neighbor 10.5.110.38 remote-as 300
 neighbor 10.5.110.42 remote-as 800
 neighbor 10.5.110.50 remote-as 1000
 neighbor 10.5.110.54 remote-as 400
```

```
 no auto-summary
!
```

3.4 Verify GDOI Encrypted Traffic between Branches

3.4.1 Verify DMVPN Tunnel Operation

During this test interfaces from GM to MPLS SP network are shutdown.

Verify DMVP tunnel operation between branches as follows:

```
demo-gm1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel10, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     2     10.5.110.38        64.0.0.3    UP 00:00:02     D
                              64.0.0.3    UP 00:00:02     D
     1     10.5.110.54        64.0.0.1    UP 23:48:30     S
```

Verify DMVPN tunnel operation between Headquarters to branches as follows:

```
demo-gm3#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel5, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1     10.5.110.34        64.0.0.2    UP    1d00h     D
     1     10.5.110.38        64.0.0.3    UP    5d00h     D
```

Verify IKE SA as follows:

```
demo-gm1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
239.192.1.190   10.5.110.88     GDOI_REKEY        1025 ACTIVE
```

Verify IPSEC SA as follows:

```
demo-gm1#show crypto ipsec sa
     PFS (Y/N): N, DH group: none
```

```
interface: Tunnel10
    Crypto map tag: demo-gdoi, local addr 10.5.110.34
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 0.0.0.0 port 848
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 20670, #pkts encrypt: 20670, #pkts digest: 20670
    #pkts decaps: 132, #pkts decrypt: 132, #pkts verify: 132
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.5.110.34, remote crypto endpt.: 0.0.0.0
     path mtu 1400, ip mtu 1400, ip mtu idb Tunnel10
     current outbound spi: 0x983E17F(159637887)
     inbound esp sas:
      spi: 0x983E17F(159637887)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2561, flow_id: Onboard VPN:561, sibling_flags 80000040, crypto
map: demo-gdoi
        sa timing: remaining key lifetime (sec): (767)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 5
        Status: ACTIVE

     outbound esp sas:
      spi: 0x983E17F(159637887)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2562, flow_id: Onboard VPN:562, sibling_flags 80000040, crypto
map: demo-gdoi
        sa timing: remaining key lifetime (sec): (767)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 5
        Status: ACTIVE
```

Verify IP route from GM1 to GM2 private network uses the DMVPN Tunnel path as follows:

```
demo-gm1#show ip route 10.5.110.209
Routing entry for 10.5.110.208/29
  Known via "eigrp 44", distance 90, metric 2306560, type internal
  Redistributing via eigrp 44
  Last update from 64.0.0.1 on Tunnel10, 1d00h ago
  Routing Descriptor Blocks:
  * 64.0.0.1, from 64.0.0.1, 1d00h ago, via Tunnel10
      Route metric is 2306560, traffic share count is 1
      Total delay is 40100 microseconds, minimum bandwidth is 2000 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
```

```
        Loading 1/255, Hops 2
```

Verify whether GM1 is receiving Multicast Keys and check the GETVPN Group information as follows:

```
*Jul 15 11:24:55 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO
from 10.5.110.88 to 239.192.1.190 with seq # 82
*Jul 15 11:25:05 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO
from 10.5.110.88 to 239.192.1.190 with seq # 83
*Jul 15 11:25:15 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO
from 10.5.110.88 to 239.192.1.190 with seq # 84
demo-gm1#show crypto gdoi
GROUP INFORMATION
    Group Name               : GETVPN-DEMO
    Group Identity           : 1357924756
    Rekeys received          : 330
    IPSec SA Direction       : Both
    Active Group Server      : 10.5.110.88
    Group Server list        : 10.5.110.88
                               10.5.110.99
    GM Reregisters in        : 522 secs
    Rekey Received(hh:mm:ss) : 00:05:12
    Rekeys received
         Cumulative          : 330
         After registration  : 330
 ACL Downloaded From KS 10.5.110.88:
   access-list  deny udp any port = 848 any port = 848
   access-list  deny tcp any any port = 23
   access-list  deny tcp any port = 23 any
   access-list  deny esp any any
   access-list  deny tcp any port = 179 any
   access-list  deny tcp any any port = 179
   access-list  deny udp any port = 500 any port = 500
   access-list  deny ospf any any
   access-list  deny eigrp any any
   access-list  deny icmp any any
   access-list  deny igmp any any
   access-list  deny pim any any
   access-list  deny ip any 224.0.0.0 0.0.255.255
   access-list  deny udp any any port = 123
   access-list  deny udp any any port = 161
   access-list  deny udp any any port = 514
   access-list  permit ip any any
KEK POLICY:
    Rekey Transport Type     : Multicast
    Lifetime (secs)          : 8169
    Encrypt Algorithm        : AES
    Key Size                 : 128
    Sig Hash Algorithm       : HMAC_AUTH_SHA
    Sig Key Length (bits)    : 1024
TEK POLICY for the current KS-Policy ACEs Downloaded:
  Tunnel10:
```

```
        IPsec SA:
            spi: 0x7E1B2606(2115708422)
            transform: esp-aes esp-sha-hmac
            sa timing:remaining key lifetime (sec): (567)
            Anti-Replay(Time Based) : 5 sec interval
```

3.4.2 Verify GDOI Encrypted Traffic between Branches

Verify traffic between branches via DMVPN tunnels are encrypted with GDOI as follows:

```
demo-gm1#show crypto ipsec sa | incl encaps
    #pkts encaps: 21442, #pkts encrypt: 21442, #pkts digest: 21442
demo-gm1#ping 10.5.110.209 source vlan 10 rep 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.5.110.209, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/28 ms
demo-gm1#show crypto ipsec sa | incl encaps
    #pkts encaps: 21542, #pkts encrypt: 21542, #pkts digest: 21542
```

3.5 Primary Network Failover Solution Test

3.5.1 Verify Primary Network Failover

Both Primary path and secondary SP network interfaces are in active state.

Create the following on **demo-pe1** to simulate primary network failure:

```
ip access-list standard block-demo-gm1
 deny   10.5.110.17
```

Before ACL is applied, traffic flows through MPLS network.

Configure netflow in interface connecting to primary and secondary SP networks as follows for verifying traffic flow via each interface during primary SP network failover:

```
demo-pe1(config)#
interface GigabitEthernet0/0
     ip route-cache flow
interface Tunnel10
    ip route-cache flow
```

Verify number of packet encrypted before the primary SP network failover as follows:

```
demo-gm1#show crypto ipsec sa | incl encap
    #pkts encaps: 5738, #pkts encrypt: 5738, #pkts digest: 5738
    #pkts encaps: 5738, #pkts encrypt: 5738, #pkts digest: 5738
```

Verify number of packets sent in each interface before the primary SP network failover as follows:

```
demo-gm1#show ip cache flow | begin SrcIf
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
```

```
Gi0/0          10.5.110.18     Null          224.0.0.13      67 0000 0000     1
Tu10           64.0.0.1        Null          224.0.0.1       02 0000 0011     1
Tu10           64.0.0.1        Null          224.0.0.10      58 0000 0000    83
Tu10           64.0.0.1        Null          239.192.1.190   02 0000 0016     1
```

Verify route from Branch 1 to Headquarters is via MPLS primary SP network as follows:

```
demo-gm1#show ip route 10.5.110.217
Routing entry for 10.5.110.216/29
  Known via "bgp 200", distance 20, metric 0
  Tag 100, type external
  Last update from 10.5.110.18 01:18:22 ago
  Routing Descriptor Blocks:
  * 10.5.110.18, from 10.5.110.18, 01:18:22 ago
      Route metric is 0, traffic share count is 1
      AS Hops 2
      Route tag 100
```

Ping corporate private network address 10.5.110.217 as follows:

```
demo-gm1#ping 10.5.110.217 source vlan 10 rep 10000
Type escape sequence to abort.
Sending 10000, 100-byte ICMP Echos to 10.5.110.217, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Meanwhile from MPLS PE device apply the following ACL to simulate the primary SP network failure in branch 1 GM (demo-gm1):

```
demo-pe1(config)#int Gi0/1
demo-pe1(config-if)#ip access-group block-demo-gm1 in
demo-pe1(config-if)#
```

Output in demo-gm1:

```
!!!!!!!!!!!U.U..U.U.U.U.U
*Jul 16 13:51:54 pst: %BGP-5-ADJCHANGE: neighbor 10.5.110.18 Down BGP Notification
received..
*Jul 16 13:52:02 pst: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 44: Neighbor 64.0.0.1
(Tunnel10) is up: new
adjacency!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 98 percent (9846/10000), round-trip min/avg/max = 1/2/48 ms
```

Traffic switched from MPLS network to DMVPN secondary SP network. This is verified with following commands.

Verify number of packet encrypted after the primary SP network failover as follows:

```
demo-gm1#show crypto ipsec sa | incl encap
    #pkts encaps: 15584, #pkts encrypt: 15584, #pkts digest: 15584
    #pkts encaps: 15584, #pkts encrypt: 15584, #pkts digest: 15584
```

Verify number of packets sent in each interface after the primary SP network failover as follows. Following output shows that packets are sent using the DMVPN tunnel interface after the primary SP network path failure in demo-gm1.

```
demo-gm1#show ip cache flow | begin SrcIf
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Tu10          64.0.0.1        Null          224.0.0.1       02 0000 0011     1
Gi0/0         10.5.110.18     Local         10.5.110.17     06 ECB5 00B3     3
Tu10          64.0.0.1        Null          224.0.0.10      58 0000 0000   365
Gi0/0         10.5.110.18     Local         10.5.110.17     01 0000 030D    13
Tu10          10.5.110.217    Local         10.5.110.201    01 0000 0000  7244
```

After the primary SP network failure, Branch 1 GM's (demo-gm1's) route to headquarters private network uses the DMVPN Tunnel interface. It is verified with the following command:

```
demo-gm1#show ip route 10.5.110.217
Routing entry for 10.5.110.216/29
  Known via "eigrp 44", distance 90, metric 1794560, type internal
  Redistributing via eigrp 44
  Last update from 64.0.0.1 on Tunnel10, 00:00:16 ago
  Routing Descriptor Blocks:
  * 64.0.0.1, from 64.0.0.1, 00:00:16 ago, via Tunnel10
      Route metric is 1794560, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 2000 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 1
```

3.5.2 Verify Primary Network Recovery and Traffic Flow Switch to Primary Network

When ACL is removed, traffic flow switches to primary MPLS SP network.

Ping corporate private network address 10.5.110.217 as follows:

```
demo-gm1#ping 10.5.110.217 source vlan 10 rep 10000
Type escape sequence to abort.
Sending 10000, 100-byte ICMP Echos to 10.5.110.217, timeout is 2 seconds:
```

Packet sent with a source address of 10.5.110.201.

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Meanwhile from MPLS PE device apply the following ACL to simulate the primary SP network path recovery in branch 1 GM (demo-gm1):

```
demo-pe1(config)#int Gi0/1
demo-pe1(config-if)#no ip access-group block-demo-gm1 in
demo-pe1(config-if)#
```

Output in Branch 1 GM (demo-gm1):

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
*Jul 16 14:46:30 pst: %BGP-5-ADJCHANGE: neighbor 10.5.110.18 Up
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (10000/10000), round-trip min/avg/max = 1/2/52 ms
```

Verify Branch 1 GM's (demo-gm1) route to headquarters private network uses MPLS SP network path via interface Gi0/1 as follows:

```
demo-gm1#show ip route 10.5.110.217
Routing entry for 10.5.110.216/29
  Known via "bgp 200", distance 20, metric 0
  Tag 100, type external
  Last update from 10.5.110.18 00:01:09 ago
  Routing Descriptor Blocks:
  * 10.5.110.18, from 10.5.110.18, 00:01:09 ago
      Route metric is 0, traffic share count is 1
      AS Hops 2
```

4. Co-op KS and GM High Availability

4.1 Objective

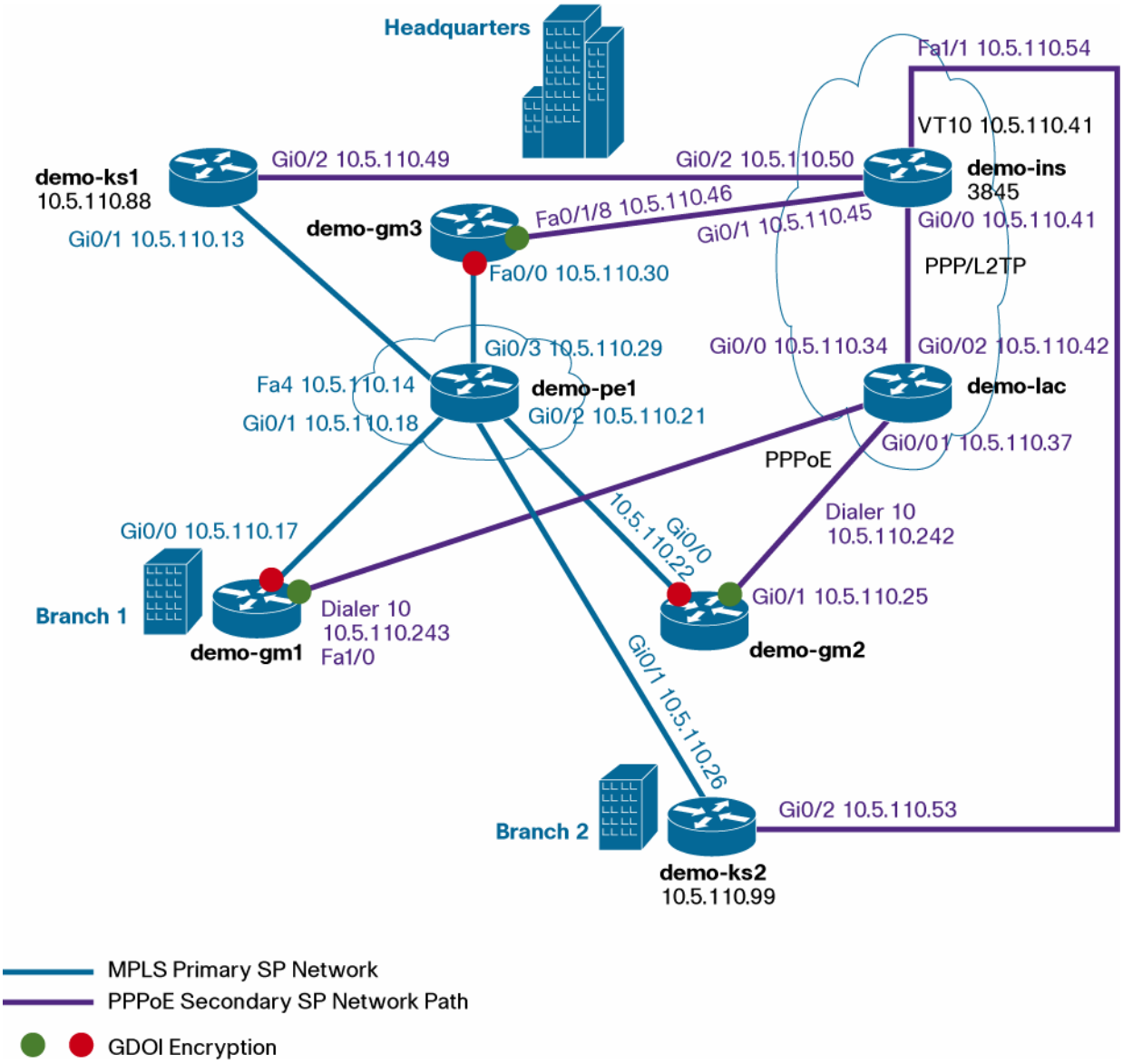
Following are objectives of the solution test.

- Test co-op KS high availability.
- Test GM high availability by using multiple GDOI groups.

4.2 Solution Test Topology

GETVPN solution test setup consists of three GMs (Group Members) and two KS (Key Server) are included in the setup. “demo-pe1” simulates the MPLS primary SP network. One Key server is located in the Headquarters. Other Key server is connected behind GM in one of the branch. Both KSs have path to primary MPLS SP network and secondary PPPoE SP network.

Figure 3. Demo GETVPN Network Topology with Multiple GDOI Groups



GMs between branches and headquarters are also connected via secondary PPPoE service provider network. This secondary network will be used when there is network outage in primary SP network. GM between branches are connected to demo-lac via PPPoE interface. PPPoL2TP tunnel connects between demo-lac and demo-lns.

GDOI encryption is done on the customer network side in the GM routers. Traffic flowing through the interface connected to primary SP network and the interface connected to the secondary service provider network are GDOI encrypted.

KS1 and KS2 are connected to both MPLS and PPPoE networks. GMs encrypt traffic using GDOI group GETVPN-DEMO-MPLS for MPLS network and encrypt traffic GETVPN-DEMO-PPPOE GDOI group for PPPoE network

Following table summarizes GDOI groups and IP addresses of GM interfaces.

Table 1. GDOI Groups and IP Addresses of GM Interfaces

GDOI Group	GDOI Encryption in demo-gm1 Interface	GDOI Encryption in demo-gm2 Interface	GDOI Encryption in demo-gm3 Interface
GETVPN-DEMO-MPLS GDOI Group for Primary MPLS Network (LAN)	Gi0/0 10.5.110.17	Gi0/0 10.5.110.22	Fa0/0 10.5.110.30
GETVPN-DEMO-PPPOE Group for Secondary SP Network (WAN)	Dialer 10 10.5.110.243	Dialer 10 10.5.110.242	Fa0/1/8 10.5.110.46

4.3 Co-op KS High Availability

If there is an outage in primary MPLS network, KS cannot send rekeys successfully to all GMs via MPLS network. This can result in Co-op KS split scenario and can cause encrypted traffic disruption between GMs. Co-op KS high availability can be improved by connecting the KSs to both primary MPLS network and secondary PPPoE network. If there is an outage in one network, rekeys will be sent via secondary network preventing disruption of encrypted traffic between GMs.

4.3.1 Verifying Co-op KS High Availability

4.3.1.1 Verifying Co-op KS Messages and Rekeys Sent via Secondary Network During MPLS Outage

To simulate outage in MPLS network, following is done.

In demo-ks2 check to make sure demo-ks1 uses route via MPLS path:

```
demo-ks2#show ip route 10.5.110.88
Routing entry for 10.5.110.88/32
  Known via "eigrp 44", distance 90, metric 158720, type internal
  Redistributing via eigrp 44
  Last update from 10.5.110.25 on GigabitEthernet0/1, 00:00:23 ago
  Routing Descriptor Blocks:
  * 10.5.110.25, from 10.5.110.25, 00:00:23 ago, via GigabitEthernet0/1
      Route metric is 158720, traffic share count is 1
      Total delay is 5200 microseconds, minimum bandwidth is 100000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
```

Make sure demo-gm1 receives rekeys from demo-gm1 by looking at the following log messages:

```
*Apr 17 12:52:50 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
MPLS from 10.5.110.88 to 239.192.1.190 with seq # 104
*Apr 17 12:52:50 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
PPPOE from 10.5.110.88 to 239.192.1.191 with seq # 104
```

```
*Apr 17 12:53:00 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
MPLS from 10.5.110.88 to 239.192.1.190 with seq # 105
*Apr 17 12:53:00 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
PPPOE from 10.5.110.88 to 239.192.1.191 with seq # 105
*Apr 17 12:53:10 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
MPLS from 10.5.110.88 to 239.192.1.190 with seq # 106
*Apr 17 12:53:10 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
PPPOE from 10.5.110.88 to 239.192.1.191 with seq # 106
```

Apply the following ACL to block traffic coming from demo-ks1 to demo-pe1 (MPLS network) in the ingress direction.

Add block-ks1-rekey ACL in demo-pe1.

```
ip access-list extended block-ks1-rekey
   deny   ip host 10.5.110.88 host 239.192.1.190
In demo-pe1 apply  the following ACL configuration as follows:
demo-pe1(config)#int Fa1/0
demo-pe1(config-if)#ip access-group block-demo-ks1 in
demo-pe1(config-if)#exit
demo-pe1(config)#exit
*Apr 17 05:19:18: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 44: Neighbor 10.5.110.13
(FastEthernet1/0) is down: holding time expired
```

Now co-op KS demo-ks2 uses route via PPPoE path to reach demo-ks1:

```
demo-ks2#show ip route 10.5.110.88
Routing entry for 10.5.110.88/32
  Known via "eigrp 88", distance 90, metric 158720, type internal
  Redistributing via eigrp 88
  Last update from 10.5.110.54 on GigabitEthernet0/2, 00:00:09 ago
  Routing Descriptor Blocks:
  * 10.5.110.54, from 10.5.110.54, 00:00:09 ago, via GigabitEthernet0/2
      Route metric is 158720, traffic share count is 1
      Total delay is 5200 microseconds, minimum bandwidth is 100000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
```

demo-gm1 will continue to receive rekeys from demo-ks1 even during MPLS network outage via PPPoE path:

```
*Apr 17 13:06:00 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
MPLS from 10.5.110.88 to 239.192.1.190 with seq # 107
*Apr 17 13:06:00 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
PPPOE from 10.5.110.88 to 239.192.1.191 with seq # 107
*Apr 17 13:06:10 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
MPLS from 10.5.110.88 to 239.192.1.190 with seq # 108
*Apr 17 13:06:10 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
PPPOE from 10.5.110.88 to 239.192.1.191 with seq # 108
*Apr 17 13:06:20 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
MPLS from 10.5.110.88 to 239.192.1.190 with seq # 109
*Apr 17 13:06:20 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
PPPOE from 10.5.110.88 to 239.192.1.191 with seq # 109
```

4.3.1.2 Verifying Co-op KS Messages and Rekeys Sent via Primary Network When MPLS Network Is Restored

To simulate MPLS network restoration, following is done:

```
demo-pe1(config)#interface FastEthernet1/0
demo-pe1(config-if)#no ip access-group block-demo-ks1 in
demo-pe1(config-if)#end
*Apr 17 06:44:27: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 44: Neighbor 10.5.110.13
(FastEthernet1/0) is up: new adjacency
```

Now co-op KS demo-ks2 uses route via primary MPLS network path to reach demo-ks1:

```
demo-ks2#show ip route 10.5.110.88
Routing entry for 10.5.110.88/32
  Known via "eigrp 44", distance 90, metric 158720, type internal
  Redistributing via eigrp 44
  Last update from 10.5.110.25 on GigabitEthernet0/1, 00:02:08 ago
  Routing Descriptor Blocks:
  * 10.5.110.25, from 10.5.110.25, 00:02:08 ago, via GigabitEthernet0/1
      Route metric is 158720, traffic share count is 1
      Total delay is 5200 microseconds, minimum bandwidth is 100000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
```

demo-gm1 will continue to receive rekeys from demo-ks1 after MPLS network restoration without any disruption to encrypted traffic flow between GMs:

```
*Apr 17 13:02:23.661: %GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for
group GETVPN-DEMO-MPLS from address 10.5.110.88 to 239.192.1.190  with seq # 20
*Apr 17 13:02:23.685: %GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for
group GETVPN-DEMO-PPPOE from address 10.5.110.88 to 239.192.1.191  with seq # 20
*Apr 17 13:02:33.685: %GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for
group GETVPN-DEMO-MPLS from address 10.5.110.88 to 239.192.1.190  with seq # 21
*Apr 17 13:02:33.709: %GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for
group GETVPN-DEMO-PPPOE from address 10.5.110.88 to 239.192.1.191  with seq # 21
*Apr 17 13:02:43.709: %GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for
group GETVPN-DEMO-MPLS from address 10.5.110.88 to 239.192.1.190  with seq # 22
*Apr 17 13:02:43.733: %GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for
group GETVPN-DEMO-PPPOE from address 10.5.110.88 to 239.192.1.191  with seq # 22
```

4.4 GM High Availability by Using Multiple GDOI Groups

It is possible GM is not able to register to KSs or receive rekey from KSs due to network problem with MPLS network. GM without GDOI keys will not be able to send and receive packets from other GMs. When this situation happens, GM is not usable.

4.4.1 Create Separate GDOI Group for Each Network

To avoid this problem, following solution is deployed.

KS1 and KS2 are connected to both MPLS and PPPoE networks. Create GDOI group GETVPN-DEMO-MPLS for MPLS network and GETVPN-DEMO-PPPOE GDOI group for PPPoE network with following CLI commands in KS1. Similar commands are entered in KS2 also.

demo-ks1:

```
crypto ipsec profile getvpn-profile
 set security-association lifetime seconds 900
 set transform-set aes128
!
crypto gdoi group GETVPN-DEMO-MPLS
 identity number 1357924756
 server local
  rekey algorithm aes 128
  rekey address ipv4 dgvpn-rekey-multicast-group
  rekey lifetime seconds 28800
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa
  sa ipsec 1
   profile getvpn-profile
   match address ipv4 sa-acl
   replay time window-size 5
  address ipv4 10.5.110.88
  redundancy
   local priority 21
   peer address ipv4 10.5.110.99
!
crypto gdoi group GETVPN-DEMO-PPPOE
 identity number 2
 server local
  rekey algorithm aes 128
  rekey address ipv4 dgvpn-rekey-multicast-group-new
  rekey lifetime seconds 28800
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa
  sa ipsec 1
   profile getvpn-profile
   match address ipv4 sa-acl
   replay time window-size 5
  address ipv4 10.5.110.88
  redundancy
   local priority 21
   peer address ipv4 10.5.110.99
!
interface Loopback0
 ip address 10.5.110.88 255.255.255.255
 ip pim sparse-mode
!
ip access-list extended dgvpn-rekey-multicast-group
 permit ip any host 239.192.1.190
ip access-list extended dgvpn-rekey-multicast-group-new
 permit ip any host 239.192.1.191
```

demo-gm1:

In GMs register to both GDOI groups and attach the GDOI group to respective interface as follows:

```
crypto gdoi group GETVPN-DEMO-MPLS
 identity number 1357924756
 server address ipv4 10.5.110.88
 server address ipv4 10.5.110.99
!
crypto gdoi group GETVPN-DEMO-PPPOE
 identity number 2
 server address ipv4 10.5.110.88
 server address ipv4 10.5.110.99
!
crypto map gdoi-mpls 1 gdoi
 set group GETVPN-DEMO-MPLS
 match address no-encryption-acl
!
crypto map gdoi-pppoe 1 gdoi
 set group GETVPN-DEMO-PPPOE
 match address no-encryption-acl
interface GigabitEthernet0/0
  crypto map gdoi-mpls
!
interface Dialer10
  crypto map gdoi-pppoe
```

4.4.2 Simulate GM Reachability Problem to Both KSs via MPLS Network

Following is done to simulate demo-gm1 reachability to KSs. Demo-gm1 gets GDOI keys from the KSs in two ways: GM gets key when it registers with KS. GM also gets key when KS sends rekey message.

4.4.2.1 Simulate GM Registration Problem with KS

Demo-gm1 registration problem with KS is simulated as follows. In demo-ks1 provide pre-share keys for all the registered interfaces except the demo-gm1 interface (10.5.110.17) connected to MPLS network as follows:

```
crypto isakmp key dGvPnPsK address 10.5.110.99
crypto isakmp key dGvPnPsK address 10.5.110.22 255.255.255.255
crypto isakmp key dGvPnPsK address 10.5.110.30 255.255.255.255
crypto isakmp key dGvPnPsK address 10.5.110.46 255.255.255.255
crypto isakmp key dGvPnPsK address 10.5.110.240 255.255.255.248
```

Similar pre-shared isakmp keys need to be provisioned in co-op KS demo-ks2 also.

demo-gm1 registration via Gi0/0 (10.5.110.17) will fail. GM will keep trying to register around TEK expiry (900 seconds for demo-gm1) forever.

```
*Apr 15 13:01:01 pst: %GDOI-4-GM_RE_REGISTER: The IPSec SA created for group
GETVPN-DEMO-MPLS may have expired/been cleared, or didn't go through. Re-register
to KS.
*Apr 15 13:01:01 pst: %CRYPTO-5-GM_REGSTER: Start registration to KS 10.5.110.88
for group GETVPN-DEMO-MPLS using address 10.5.110.17
*Apr 15 13:01:01 pst: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Informational mode
failed with peer at 10.5.110.88
*Apr 15 13:01:41 pst: %CRYPTO-5-GM_CONN_NEXT_SER: GM is connecting to next key
server from the list
```

```
*Apr 15 13:01:41 pst: %CRYPTO-5-GM_REGSTER: Start registration to KS 10.5.110.99
for group GETVPN-DEMO-MPLS using address 10.5.110.17
```

4.4.2.2 Simulate GM Not Receiving Rekeys from KS

Following is done to simulate GM not receiving rekeys from KS.

Add the following ACL in demo-pe1:

```
ip access-list extended block-ks1-rekey-to-gm1
   deny   ip host 10.5.110.88 host 239.192.1.190
   deny   ip host 10.5.110.99 host 239.192.1.190
   permit ip any any
```

Attach this ACL to the demo-pe1 interface connecting to demo-gm1 in the MPLS network as follows:

```
interface GigabitEthernet0/1
  description connected to demo-gm1
  ip access-group block-ks1-rekey-to-gm1 out
```

This will block GETVPN-DEMO-MPLS keys sent via MPLS cloud to demo-gm1. demo-gm1 will not have GDOI keys for GETVPN-DEMO-MPLS network.

```
demo-gm1#show crypto gdoi
GROUP INFORMATION
    Group Name               : GETVPN-DEMO-MPLS
    Group Identity           : 1357924756
    Rekeys received          : 0
    IPSec SA Direction       : Both
    Active Group Server      : 10.5.110.88
    Group Server list        : 10.5.110.88
                               10.5.110.99
    GM Reregisters in        : 0 secs
    Rekey Received(hh:mm:ss) : 1d19h
    Rekeys received
         Cumulative          : 0
         After registration  : 1
 ACL Downloaded From KS 10.5.110.88:
TEK POLICY:
  GigabitEthernet0/0:
```

Demo-gm1 will receive rekeys for GETVPN-DEMO-PPPOE network:

```
*Apr 15 12:57:54 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
PPPOE from 10.5.110.88 to 239.192.1.191 with seq # 59
*Apr 15 12:58:04 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
PPPOE from 10.5.110.88 to 239.192.1.191 with seq # 60
*Apr 15 12:58:14 pst: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GETVPN-DEMO-
PPPOE from 10.5.110.88 to 239.192.1.191 with seq # 61
```

4.4.3 Resolve Routing Problems in demo-gm1 by Blocking Routes

Demo-gm1 routes are still pointing to the MPLS network. However demo-gm1 does not have GDOI keys to encrypt traffic over MPLS network. Traffic from demo-gm1 to other GMs will be dropped because there are no keys;

however, the policy indicates encryption is required. Likewise, traffic from other GM's to demo-gm1 will fail since traffic arriving at demo-gm1 will be encrypted and demo-gm1 does not have the appropriate GDOI keys.

Ping demo-gm2 MPLS and PPPoE IP address as follows:

```
demo-gm1#ping 10.5.110.22 source vlan 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.110.22, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
....
Success rate is 0 percent (0/4)
demo-gm1#ping 10.5.110.242 source vlan 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.110.242, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
...
Success rate is 0 percent (0/3)
```

Following display shows route to demo-gm2 from demo-gm1. It forwards packet via MPLS PE address.

```
demo-gm1#show ip route 10.5.110.22
Routing entry for 10.5.110.20/30
  Known via "eigrp 44", distance 90, metric 3072, type internal
  Redistributing via eigrp 44
  Last update from 10.5.110.18 on GigabitEthernet0/0, 00:05:57 ago
  Routing Descriptor Blocks:
  * 10.5.110.18, from 10.5.110.18, 00:05:57 ago, via GigabitEthernet0/0
      Route metric is 3072, traffic share count is 1
      Total delay is 20 microseconds, minimum bandwidth is 1000000 Kbit
      Reliability 254/255, minimum MTU 1500 bytes
      Loading 1/255, Hops
D       10.5.110.20/30 [90/3072] via 10.5.110.18, 00:07:20, GigabitEthernet0/0
```

demo-gm2 has the GDOI key and demo-gm1 does not have GDOI key. To verify you can do the following.

From demo-gm2, ping demo-gm1's MPLS LAN IP address as follows:

```
demo-gm2#ping 10.5.110.17 source vlan 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.110.17, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.209
.....
Success rate is 0 percent (0/5)
```

On demo-gm1 you will see the following log message indicating it does not have the GDOI key.

```
demo-gm1#
*Apr 16 11:57:07 pst: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has
invalid spi for destaddr=10.5.110.17, prot=50, spi=0x75D10654(1976632916),
srcaddr=10.5.110.209
```

Following log message in demo-gm1 indicates failure of GM registration with last co-op KS:

```
*Apr 15 13:01:01 pst: %CRYPTO-5-GM_REGSTER: Start registration to KS 10.5.110.99
for group GETVPN-DEMO-MPLS using address 10.5.110.17
*Apr 15 13:01:01 pst: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Informational mode
failed with peer at 10.5.110.99
```

When GM registration fails to last Co-op KS, one needs to block all routes to the other GMs while accepting routes to the KSs via MPLS network path.

One way to do this is as follows.

In the GM (demo-gm1) which is having registration problem, add the following ACL:

```
access-list 17 permit 10.5.110.88
access-list 17 permit 10.5.110.99
access-list 17 deny   any
```

In demo-gm1 use following Embedded Event Manager (EEM) configuration CLIs to block all routes to the other GMs while accepting routes to the KSs via MPLS network path.

```
event manager applet block-lan-routes-except-ks
 event syslog pattern "%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Informational
mode failed with peer at 10.5.110.99"
 action 1 cli command "enable"
 action 2 cli command "configure terminal"
 action 3 cli command "router eigrp 44"
 action 4 cli command "distribute-list 17 in"
```

The above EEM commands will be automatically executed during run-time to block routes whenever GM (demo-gm1) fails to register with KS (demo-ks1). This will result in blocking all the routes to the other GMs while accepting routes to KSs via MPLS network path. Now demo-gm1 can send and receive encrypted traffic from other GMs using GETVPN-DEMO-PPPOE GDOI keys using PPPoE network path.

After EEM applet runs, following is EIGRP related running-config of demo-gm1:

```
router eigrp 44
 network 10.5.110.16 0.0.0.3
 network 10.5.110.200 0.0.0.7
 distribute-list 17 in
 no auto-summary
!
router eigrp 88
 network 10.5.110.200 0.0.0.7
 network 10.5.110.240 0.0.0.7
 no auto-summary
!
```

Verify successful blocking of routes via MPLS network as follows.

Ping demo-gm2 Dialer interface from demo-gm1:

```
demo-gm1#ping 10.5.110.242 source vlan 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.110.242, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Ping demo-gm2 LAN interface from demo-gm1:

```
demo-gm1#ping 10.5.110.22 source vlan 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.110.22, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

Verify routes are forwarding traffic to PPPoE network:

```
demo-gm1#show ip route
Gateway of last resort is 10.5.110.41 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 15 subnets, 3 masks
D       10.5.110.99/32
           [90/156416] via 10.5.110.18, 03:55:47, GigabitEthernet0/0
D       10.5.110.88/32
           [90/156416] via 10.5.110.18, 04:25:45, GigabitEthernet0/0
D       10.5.110.32/30 [90/46228992] via 10.5.110.41, 04:43:53
D       10.5.110.36/30 [90/46228992] via 10.5.110.41, 04:43:53
C       10.5.110.41/32 is directly connected, Dialer10
D       10.5.110.40/30 [90/46226432] via 10.5.110.41, 04:43:53
D       10.5.110.44/30 [90/46228736] via 10.5.110.41, 04:43:54
D       10.5.110.48/30 [90/46228736] via 10.5.110.41, 04:41:32
D       10.5.110.52/30 [90/46228736] via 10.5.110.41, 04:39:15
C       10.5.110.16/30 is directly connected, GigabitEthernet0/0
C       10.5.110.243/32 is directly connected, Dialer10
D       10.5.110.242/32 [90/48786176] via 10.5.110.41, 04:44:00
C       10.5.110.200/29 is directly connected, Vlan10
D       10.5.110.208/29 [90/48788736] via 10.5.110.41, 00:00:14
D       10.5.110.216/29 [90/46231296] via 10.5.110.41, 00:00:14
D*EX 0.0.0.0/0 [170/46231296] via 10.5.110.41, 00:00:14
```

Every time around the TEK expiry time (~ 900 secs) you will see the following registration failure:

```
*Apr 15 13:57:01 pst: %GDOI-4-GM_RE_REGISTER: The IPSec SA created for group
GETVPN-DEMO-MPLS may have expired/been cleared, or didn't go through. Re-register
to KS.
*Apr 15 13:57:01 pst: %CRYPTO-5-GM_REGSTER: Start registration to KS 10.5.110.88
for group GETVPN-DEMO-MPLS using address 10.5.110.17
*Apr 15 13:57:01 pst: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Informational mode
failed with peer at 10.5.110.88
```

All traffic from demo-gm1 will be encrypted and sent via PPPoE interface using GETVPN-MPLS-PPOE GDOI group due to invocation of **EEM applet block-lan-routes-except-ks**. demo-gm1 will be able to receive and send traffic from other GMs.

4.4.4 Unblock Block Routes When GM to KS Network Reachability Is Restored

Demo-gm1 to demo-ks1 network reachability is restored by undoing steps done in section 3.2 as follows.

Add following configuration to demo-ks1 and demo-ks2:

```
crypto isakmp key dGvPnPsK address 10.5.110.17 255.255.255.255
```

to allow demo-gm1 registration using pre-shared keys.

In demo-pe1 remove the access-list to block rekeys from KS1 to demo-gm1:

```
demo-pe1(config)#interface GigabitEthernet0/1
demo-pe1(config-if)#no ip access-group block-ks1-rekey-to-gm1 out
demo-pe1(config-if)#end
```

When the TEK time expires in demo-gm1, demo-gm1 will successfully register with the first KS.

```
*Apr 15 15:39:42 pst: %CRYPTO-5-GM_REGSTER: Start registration to KS 10.5.110.88
for group GETVPN-DEMO-MPLS using address 10.5.110.17
*Apr 15 15:39:51 pst: %GDOI-5-GM_REGS_COMPL: Registration to KS 10.5.110.88
complete for group GETVPN-DEMO-MPLS using address 10.5.110.17
```

Traffic from demo-gm1 to other GMs are still getting forwarded via PPPoE secondary network due to blocking of MPLS routes in demo-gm1 due to **block-*lan-routes-except-ks* EEM** applet.

Traffic from demo-gm1 to demo-gm2 goes via PPPoE secondary network.

```
demo-gm1#show ip route 10.5.110.22
Routing entry for 10.5.110.20/30
  Known via "eigrp 44", distance 90, metric 48786432, type internal
  Redistributing via eigrp 44
  Last update from 10.5.110.41 02:04:44 ago
  Routing Descriptor Blocks:
  * 10.5.110.41, from 10.5.110.41, 02:04:44 ago
      Route metric is 48786432, traffic share count is 1
      Total delay is 120010 microseconds, minimum bandwidth is 56 Kbit
      Reliability 254/255, minimum MTU 1492 bytes
      Loading 1/255, Hops 2
```

Now demo-gm1 reachability with first co-op KS demo-ks1 via primary MPLS network is restored, unblock the routes filter applied in section 3.3 by applying the following EEM applet *unblock-lan-routes* CLIs in demo-gm1:

```
event manager applet unblock-lan-routes
 event syslog pattern " %GDOI-5-GM_REGS_COMPL: Registration to KS 10.5.110.88
complete for group GETVPN-DEMO-MPLS using address 10.5.110.17"
 action 1 cli command "enable"
 action 2 cli command "configure terminal"
```

```
 action 3 cli command "router eigrp 44"
 action 4 cli command "no distribute-list 17 in"
```

Verify to make sure demo-gm1 traffic to other GMs goes through primary MPLS network.

Verify demo-gm2 route from demo-gm1:

```
demo-gm1#show ip route 10.5.110.22
Routing entry for 10.5.110.20/30
  Known via "eigrp 44", distance 90, metric 3072, type internal
  Redistributing via eigrp 44
  Last update from 10.5.110.18 on GigabitEthernet0/0, 00:01:53 ago
  Routing Descriptor Blocks:
  * 10.5.110.18, from 10.5.110.18, 00:01:53 ago, via GigabitEthernet0/0
      Route metric is 3072, traffic share count is 1
      Total delay is 20 microseconds, minimum bandwidth is 1000000 Kbit
      Reliability 254/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Ping demo-gm2 Dialer10 interface from demo-gm1:

```
demo-gm1#ping 10.5.110.242 source vlan 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.110.242, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

Ping demo-gm2 MPLS LAN IF from demo-gm1:

```
demo-gm1#ping 10.5.110.22 source vlan 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.110.22, timeout is 2 seconds:
Packet sent with a source address of 10.5.110.201
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

5. Glossary

The following list describes acronyms and definitions for terms used throughout this document:

GETVPN	Group Encrypted Transport. A scalable VPN using group technology.
GDOI	Group Domain of Interpretation, RFC 3547. A group key management system that is complimentary to IKE.
IKE	Internet Key Exchange, RFC 2409. A pair-wise key management system used to negotiation IPSec tunnels.
IPSec	IP Protocol Security, RFC 2401. The common name for a set of protocols that protect IP packets.
ISAKMP	Internet Security Association and Key Management Protocol, RFC 2408. ISAKMP defines payloads for exchanging key generation and authentication data.
SA	Security Association. SAs contain all the information required for execution of various network security services, such as the IP layer services (such as header authentication and payload encapsulation), transport or application layer services, or self-protection of negotiation traffic.
GM	Group Member
KS	Key Server
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
LNS	Layer 2 Network Server
LAC	Layer 2 Access Concentrator
L2TP	Layer 2 Tunneling Protocol

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-617021-00 08/10